nCrypted Cloud

Mac OSX User Manual

Version 2.0

Welcome to nCrypted Cloud!

nCrypted Cloud is a **Privacy, Security, and Collaboration** application that uses Industry Standard Encryption Technology (AES-256 bit encryption) to secure files stored in the cloud.

Through seamless cloud integration, nCrypted Cloud acts as a layer on top of cloud storage services, giving you the ability to protect data, securely share and collaborate with anyone, and keep track of all data activity.

Users must have a cloud storage account before using nCrypted Cloud. nCrypted Cloud Cloud is compatible with **Dropbox, Google Drive, One Drive, Box, and Egnyte**.

This user guide will show you how to use nCrypted Cloud's on your Mac OSX machine.

Table of Contents

1 Getting Started

1.1 Register.....3
1.2 Download.....5
1.3 Access.....7

2 Preferences

2.1 General.....8
2.2 Account.....12
2.3 Proxy.....13
2.4 Support.....14

3 Cloud Storage

3.1 Connect Your Cloud.....15

4 Identities

4.1 Add Corporate Identity.....18
4.2 Swtich Identities.....21

5 Secure

5.1 Make Private.....22
5.2 Remove Privacy.....23
5.3 Copy Unrotected.....24
5.4 Apply Sensitivity.....26

6 Trusted Sharing

6.1 How To Trusted Share.....28
6.2 Trusted Share Process.....32

7 Share Securely

7.1 How To Share Securely 36
7.2 View Shared With.....38
7.3 Remove User Access.....39
7.4 Open/Closed Enrollment.....40
7.5 Remove/Enable Shared Access.....42

8 Auditing

8.1 View Auditing Events.....44

Getting Started

1

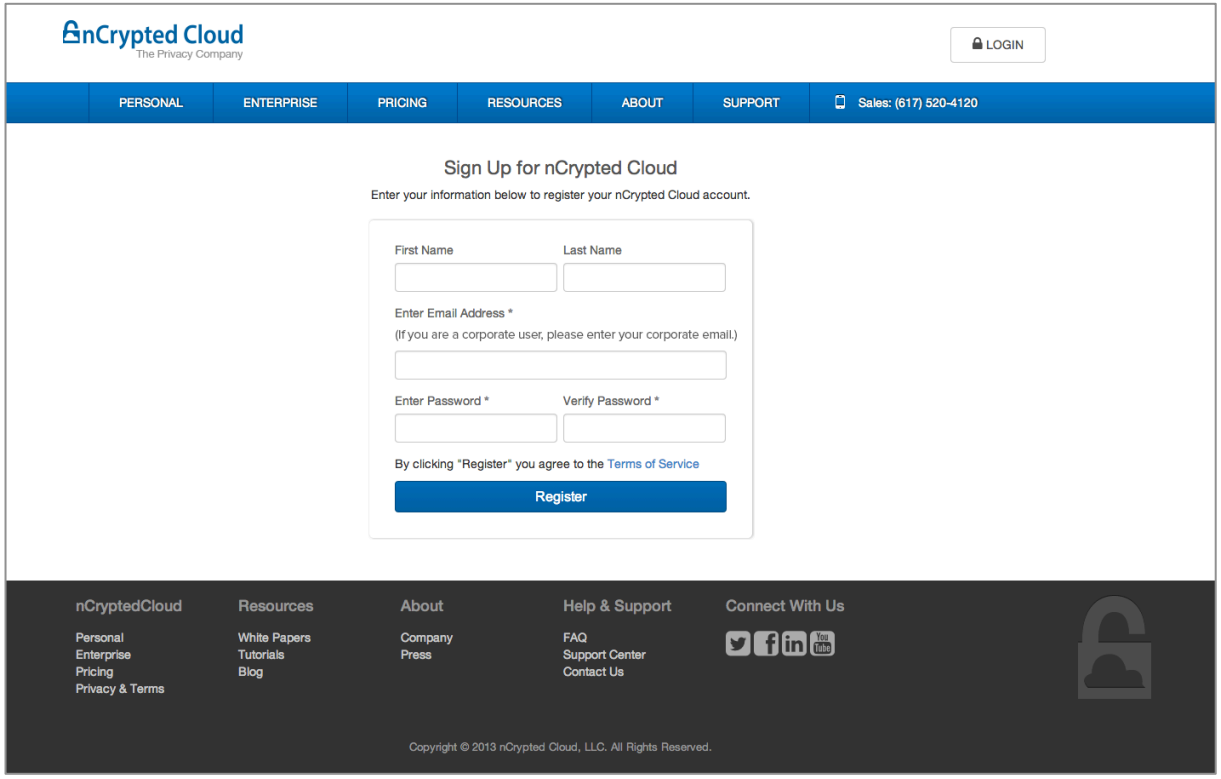
Getting Started

1.1

Register for nCrypted Cloud

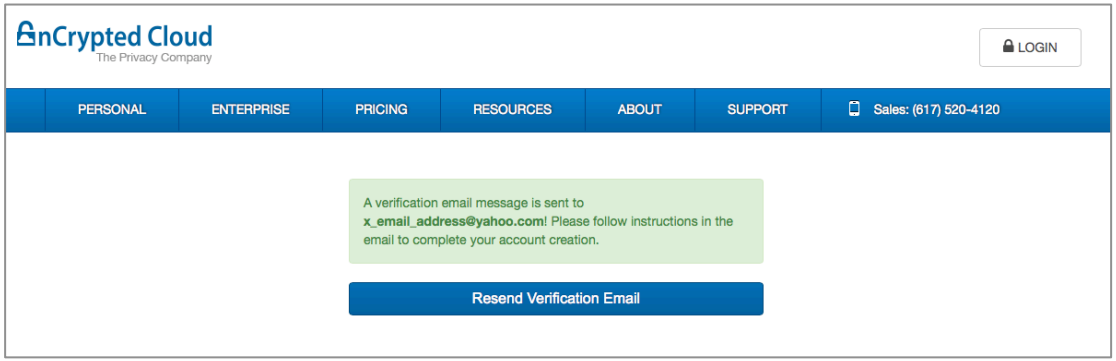
1. Go to www.ncryptedcloud.com and click the “Sign Up” button in the top right corner of the page

2. Fill in the registration information below: First Name, Last Name, Email, Password

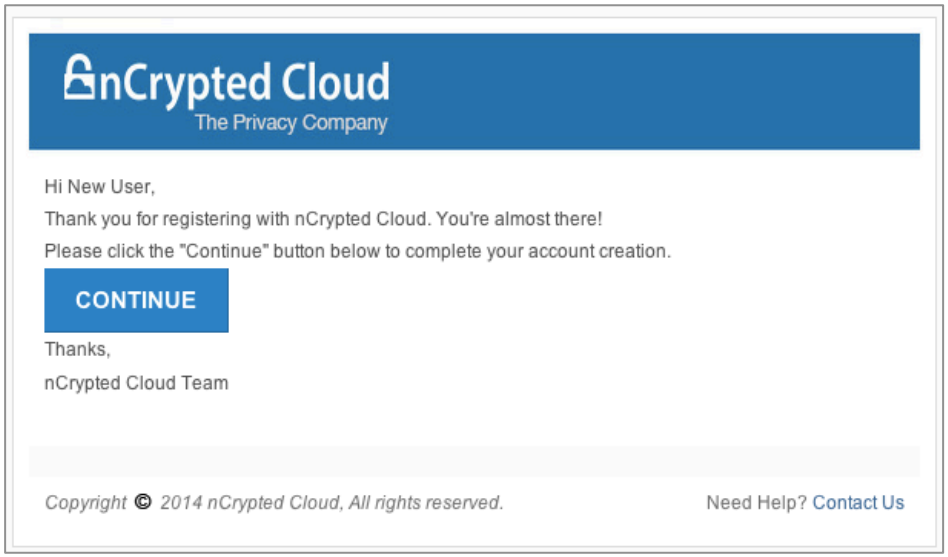


Getting Started
1.1

3. Registration is complete! You will receive an email to verify your account.



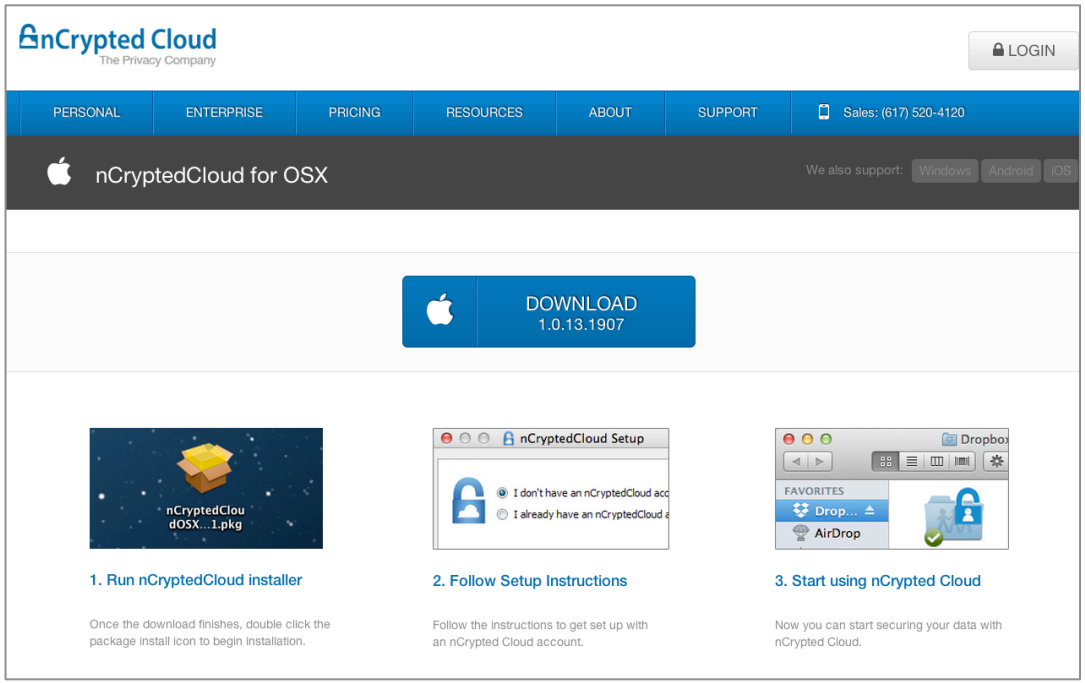
4. This is the verification email you will receive. Click “Continue” to verify your email.


nCrypted Cloud
The Privacy Company
Hi New User,
Thank you for registering with nCrypted Cloud. You're almost there!
Please click the "Continue" button below to complete your account creation.
CONTINUE
Thanks,
nCrypted Cloud Team
Copyright © 2014 nCrypted Cloud, All rights reserved.
Need Help? Contact Us

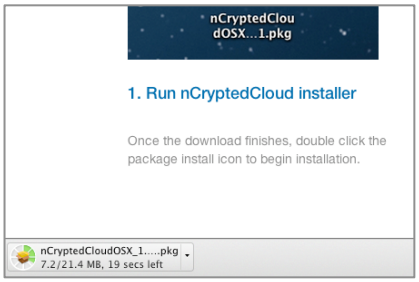
Getting Started
1.2

Download nCrypted Cloud

1. Go to the nCrypted Cloud Download Page: www.ncryptedcloud.com/download



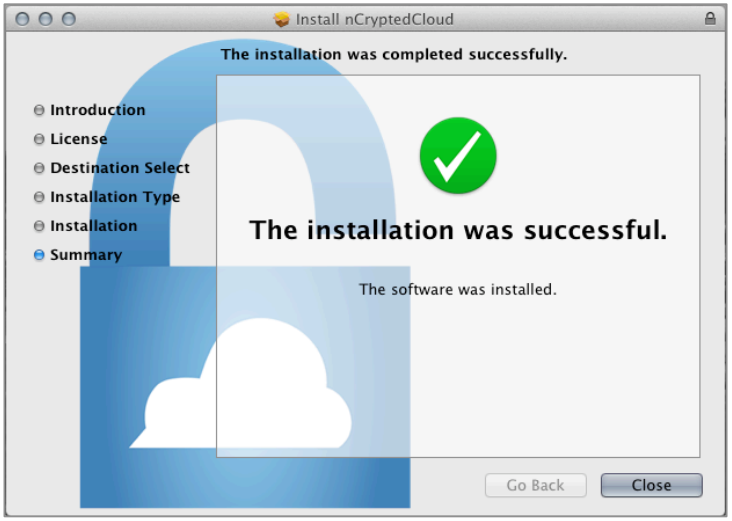
2. Click “Download” and the Install Package will run


nCryptedClou
dOSX...1.pkg
1. Run nCryptedCloud installer
Once the download finishes, double click the package install icon to begin installation.
nCryptedCloudOSX_1.....pkg
7.2/21.4 MB, 19 secs left

Getting Started
1.2

3. Once the install package is fully downloaded, double-click the file and begin the installation process.

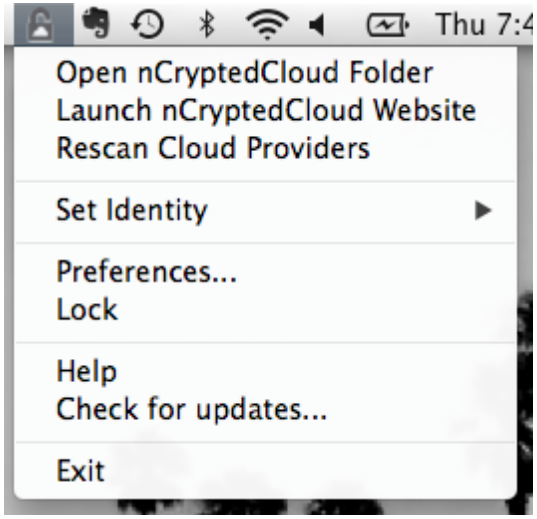
4. Once you accept nCrypted Cloud's Terms of Service, choose an install destination, and confirm the installation, nCrypted Cloud will be installed.



Getting Started
1.3

Access nCrypted Cloud

Now that nCrypted Cloud is downloaded on your machine, you can access nCrypted Cloud by clicking on the lock icon in your taskbar.



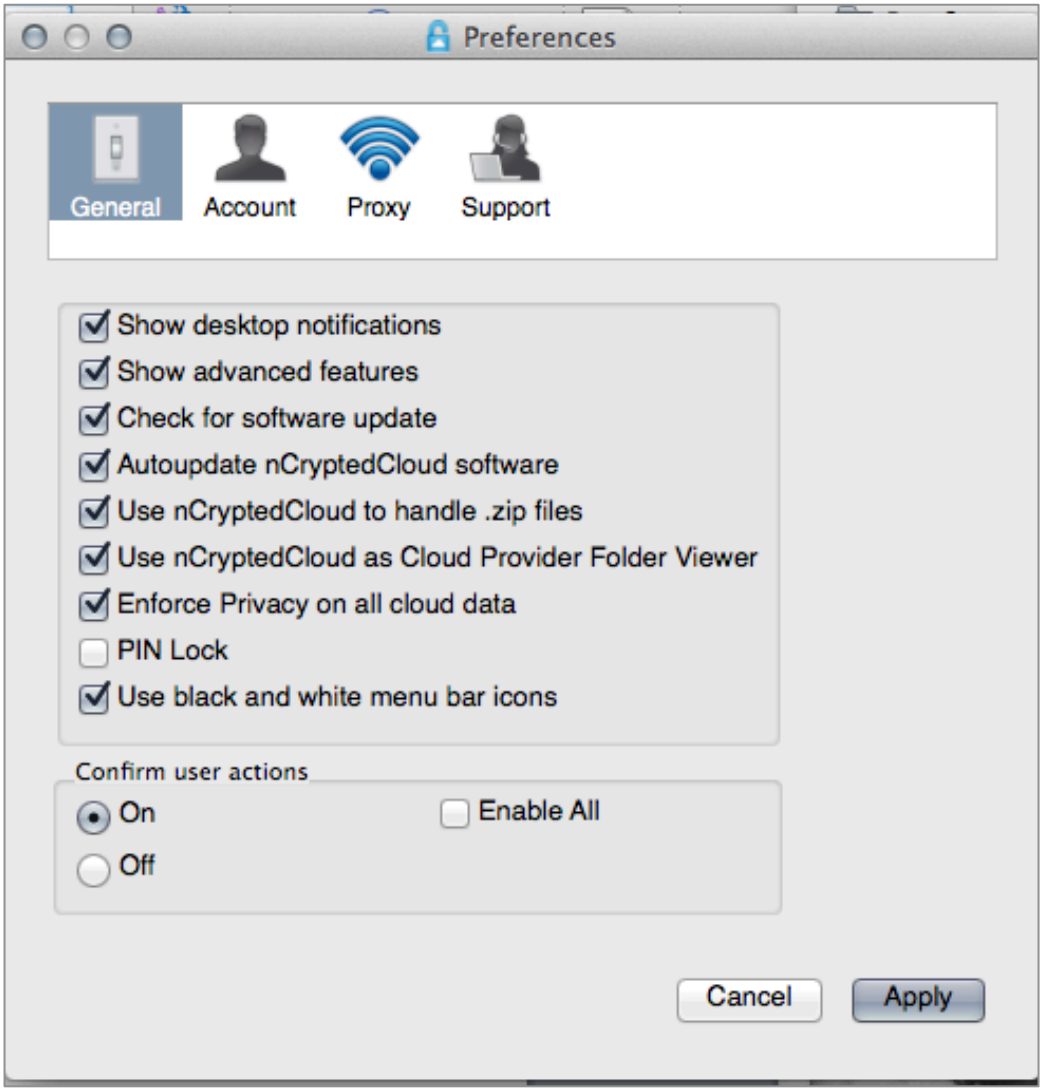
From this drop-down menu, you have the ability to open nCrypted Cloud on your desktop, launch the nCrypted Cloud Web Portal, scan your computer for undetected Cloud Providers, set your identity, adjust your preferences, lock nCrypted Cloud, get help, and check for updates.

2 Preferences

Preferences 2.1

General

Before using nCrypted Cloud, it is important to make sure that your settings are properly adjusted. These next few pages will go over each setting in your Preferences Menu in detail.

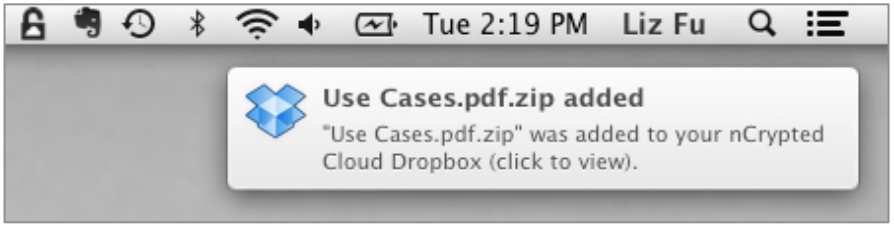


Preferences 2.1

General

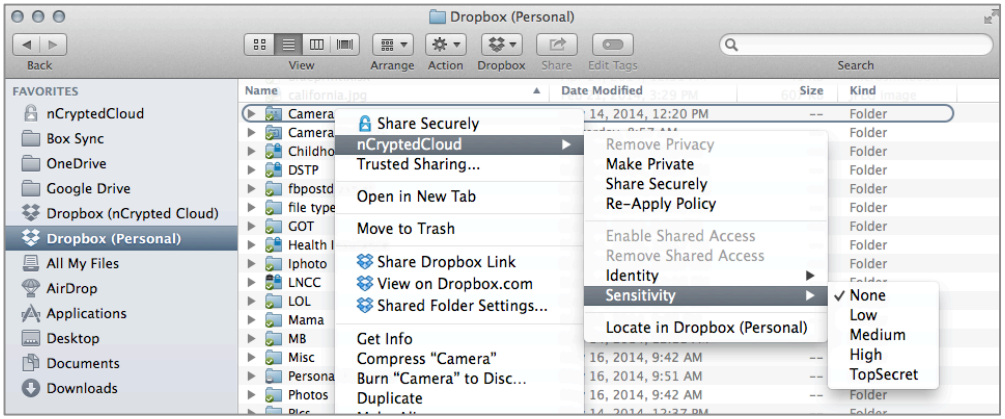
1. Show desktop notifications:

   Receive pop-up notifications every time a change is made to your cloud.



2. Show advanced features:

   This gives you the ability to apply sensitivity (low, medium, high, top secret) to your folders. By applying sensitivity, you can see right on the folder



3. Check for software updates:

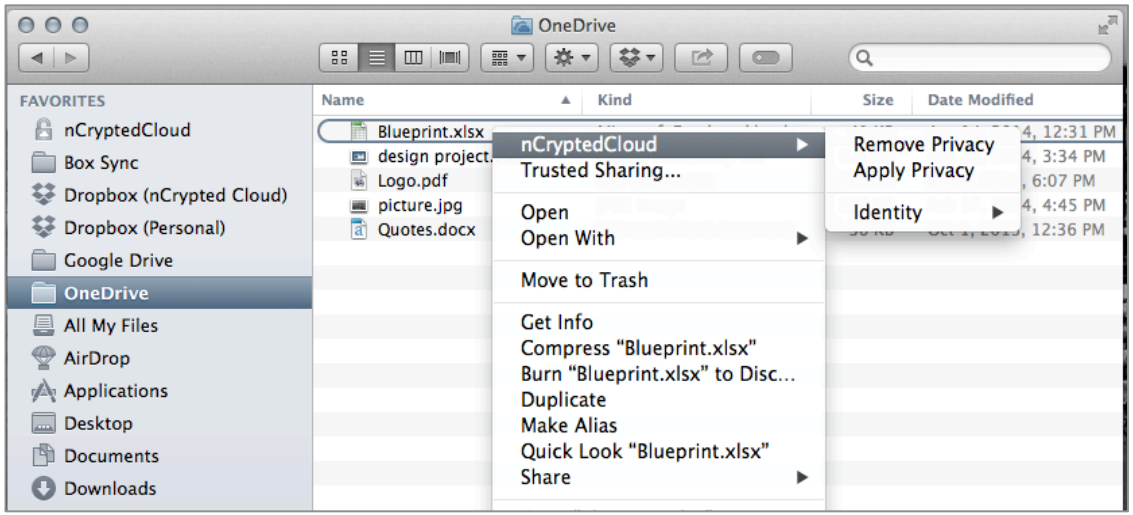
   This option will notify you when a new version of nCrypted Cloud is available for download.

Preferences 2.1

4. Auto-update nCrypted Cloud software:
   Automatically update to the latest version of nCrypted Cloud

5. Use nCrypted Cloud to handle .zip files:
   Open any .zip files using nCrypted Cloud. When files are encrypted, the file changes from its original format (.doc, .pdf, .xls, .psd) to a .zip file format. Files encrypted with nCrypted Cloud can only be accessed using nCrypted Cloud. This setting will ensure that you can easily open encrypted files.

6. Use nCrypted Cloud as Cloud Provider Folder Viewer:
   This setting makes nCrypted Cloud your default cloud provider viewer. This means that when you open Dropbox, Google Drive, Box, One Drive, and Egnyte on your desktop, nCrypted Cloud is seamlessly integrated.

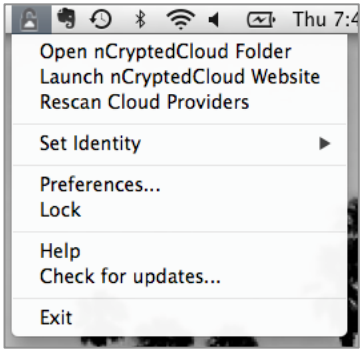


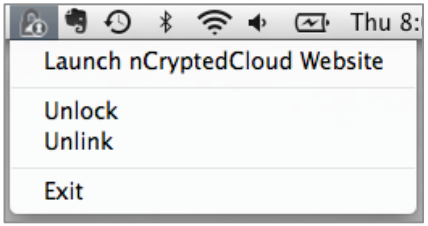
7. Enforce Privacy on all cloud data:
   Encrypt all data stored in your cloud.

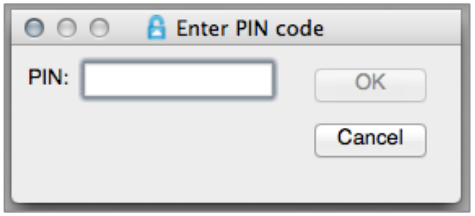
Preferences 2.1

8. PIN Lock:

   Require a PIN to access nCrypted Cloud. In order to enable this setting on the desktop client, you must first set a person PIN either on the Web Portal or Mobile App. Once you do so, you can enforce the PIN code by selecting “Lock” from the drop-down menu. nCrypted Cloud will no longer be accessible on this machine. When you click on the icon now, this is the new drop-down menu you will see. When you select “Unlock” or “Launch nCrypted Cloud Website” you will be asked to enter your pin before proceeding. Once you do so, nCrypted Cloud will run just as it normally would.



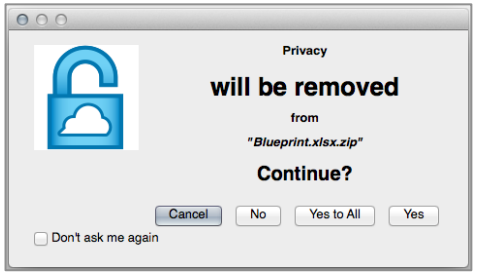




9. Use black and white menu bar icons:

   Make the nCrypted Cloud Icon in your toolbar black.

10. Confirm user actions: are you sure you want to do this



On: Receive confirmation pop-up windows for every action.

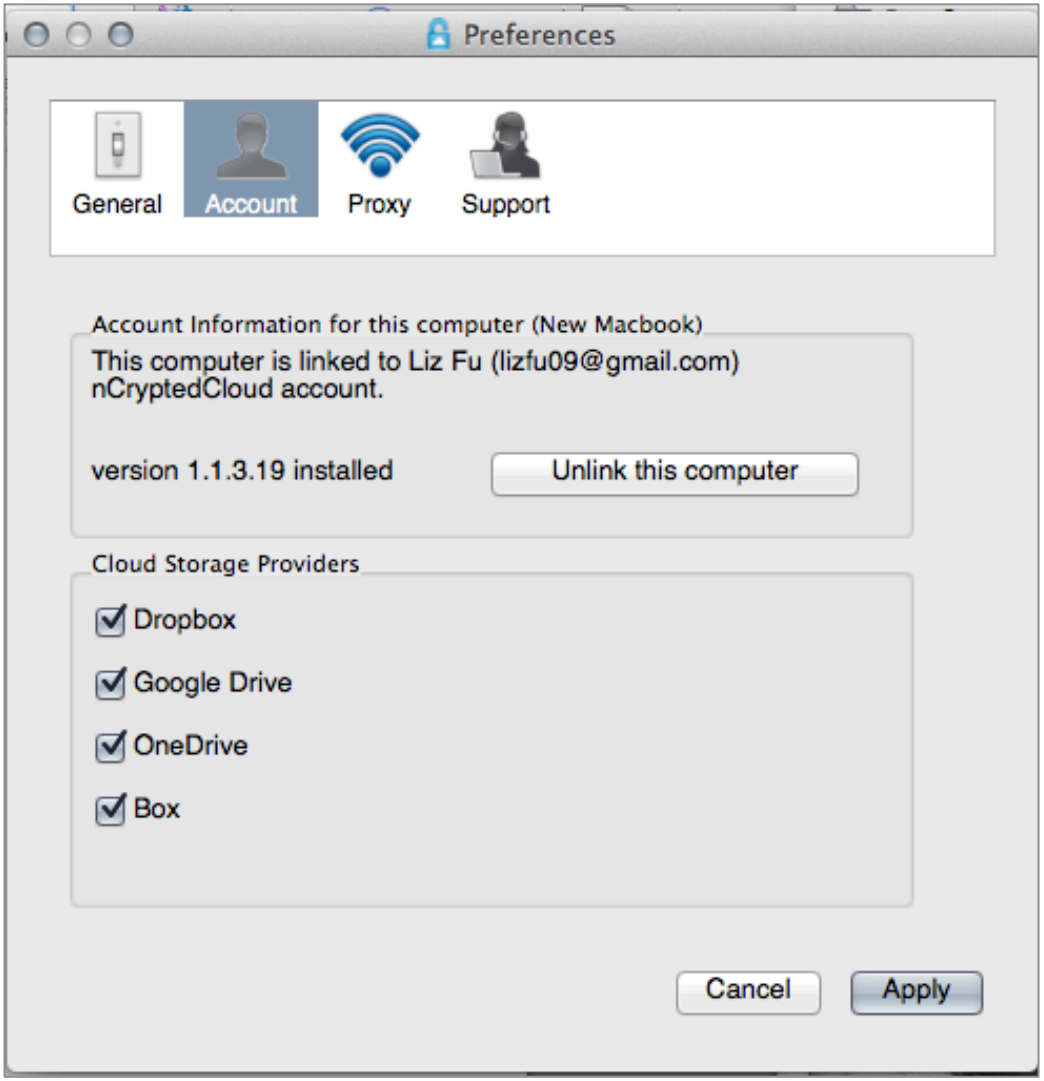
Off: Don’t receive confirmation pop-up windows.

Enable All: Allow all actions without confirmation pop-up.

Preferences 2.2

Account

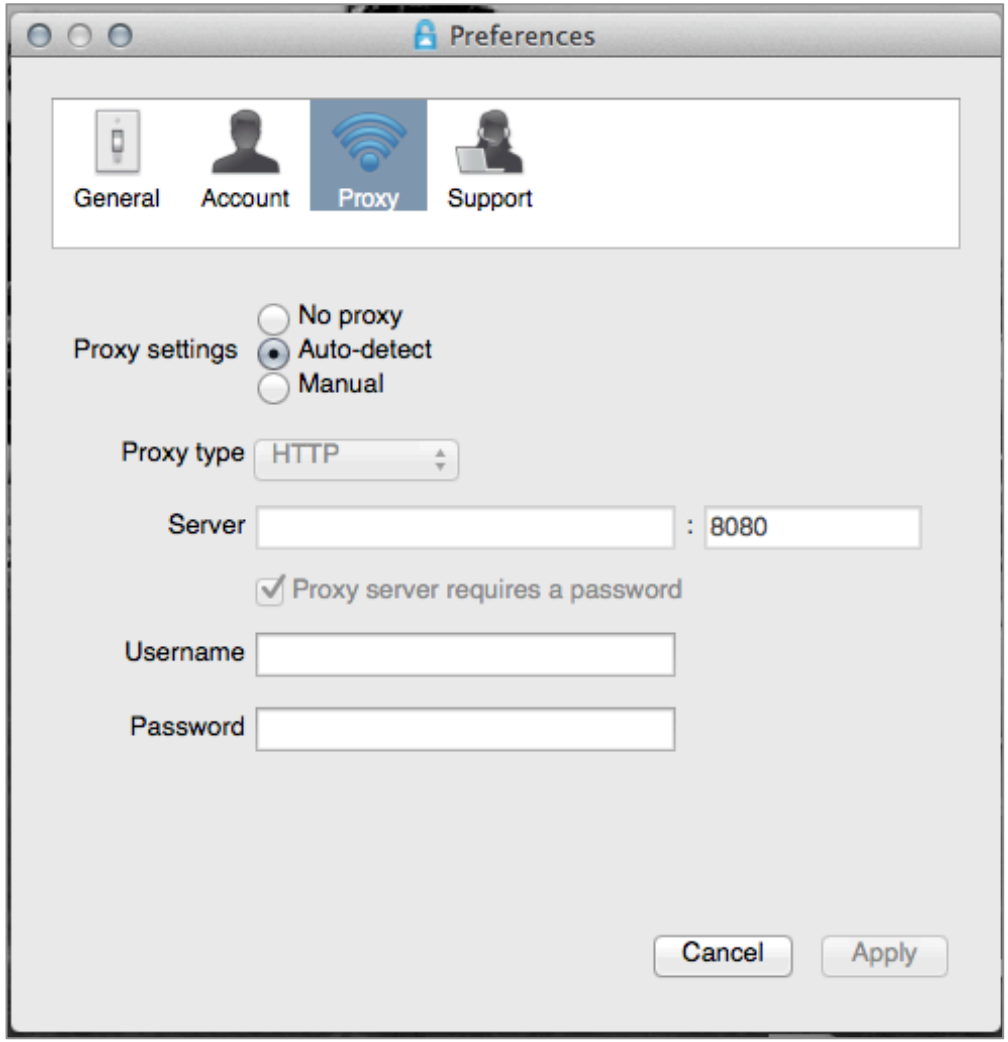
The Account tab in your Preferences is where you go to connect cloud providers and unlink nCrypted Cloud from your computer. When you unlink nCrypted Cloud, nCrypted Cloud will be removed from your machine.



Preferences 2.3

Proxy

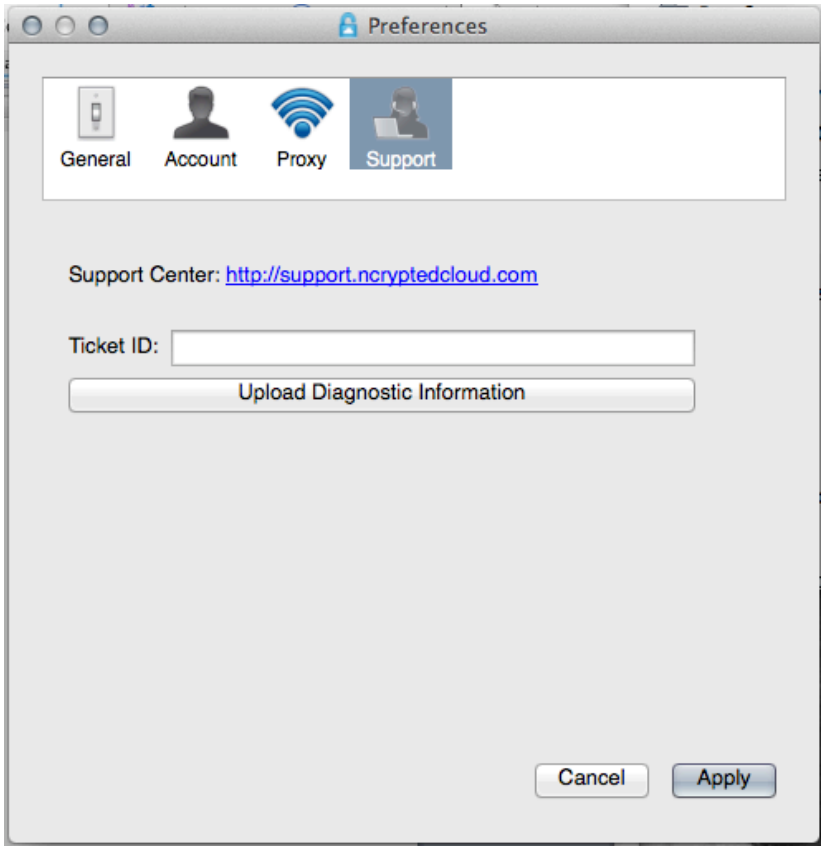
The Proxy tab gives you the ability to customize your proxy settings.



Preferences 2.4

Support

If you ever have any issues with our software, you can go to the Support Tab in your preferences and submit a request. The Support Center Link will redirect you to our support page where you can submit a ticket with a description of the issue you are having. Once you complete the form, you will receive a ticket number.



If you would like to upload your machine's diagnostic information so our team can investigate this information and get to the bottom of your issue, enter your ticket number in the "Ticket ID" section and click Upload Diagnostic Information. Our Team will receive this information and assess the problem immediately.

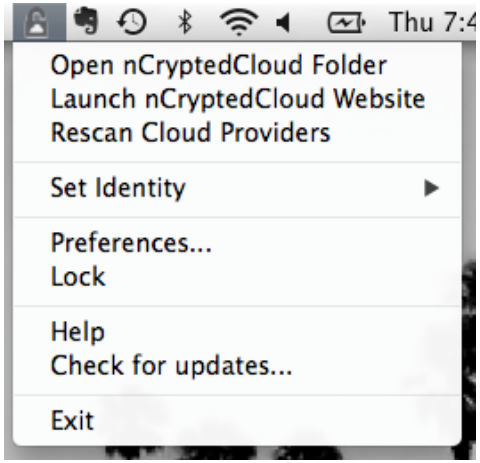
Cloud Storage

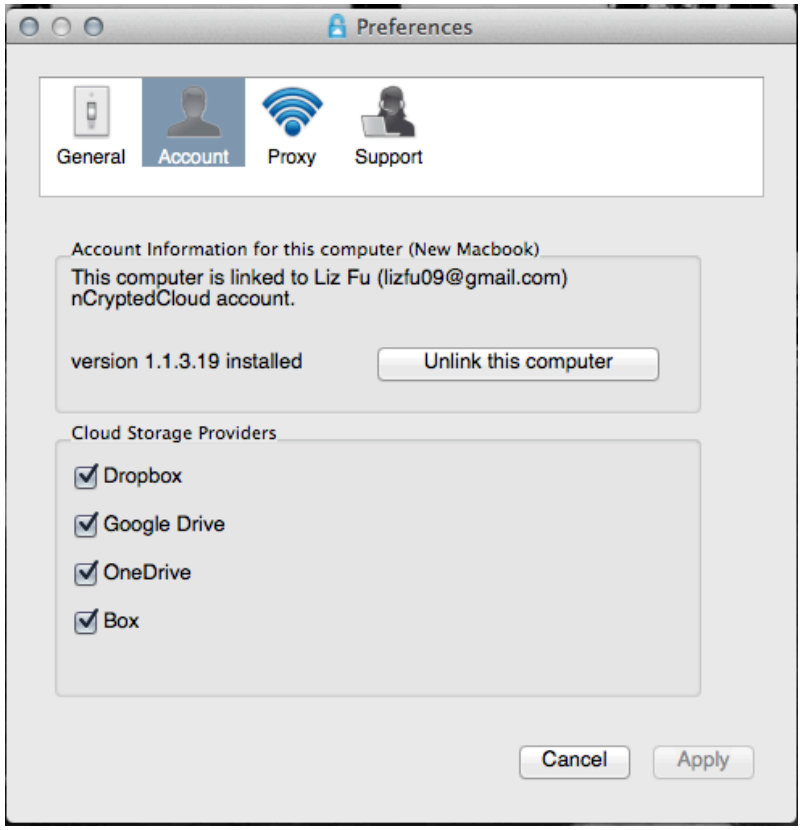
3

Cloud Storage 3.1

Connect Your Cloud

To sync cloud providers to nCrypted Cloud, click the nCrypted Cloud icon in your taskbar and select "Preferences" from the drop-down menu. Go to the "Account" tab and check the boxes next to the cloud providers you wish to sync. Once these boxes are checked, nCrypted Cloud will automatically sync with these cloud providers.

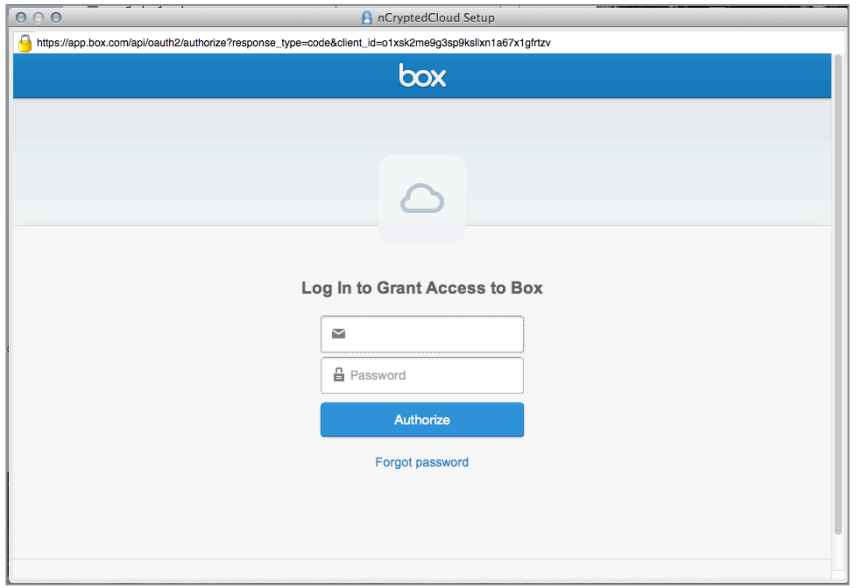


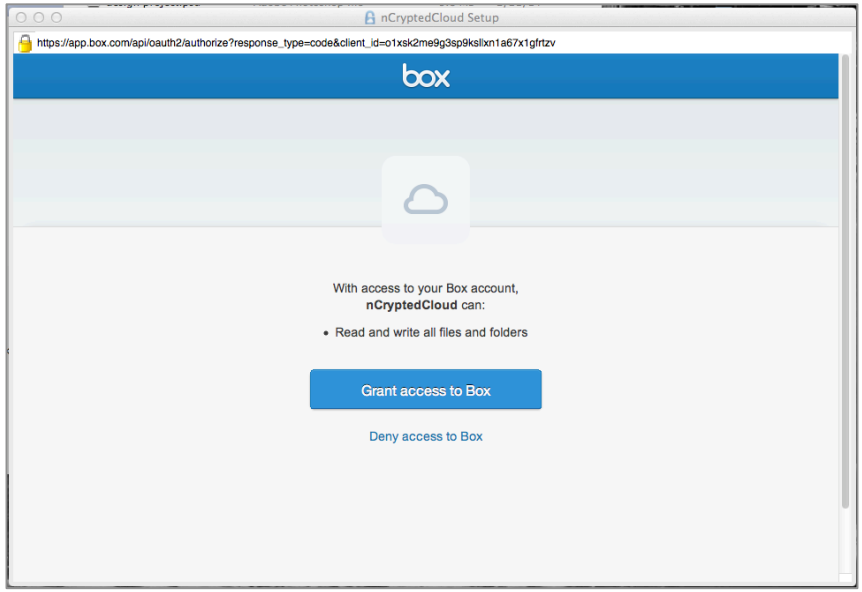


If you just installed a new cloud storage service on your desktop and nCrypted Cloud did not automatically connect to this cloud, select "Rescan Cloud Providers" from the drop-down menu.

Cloud Storage 3.1

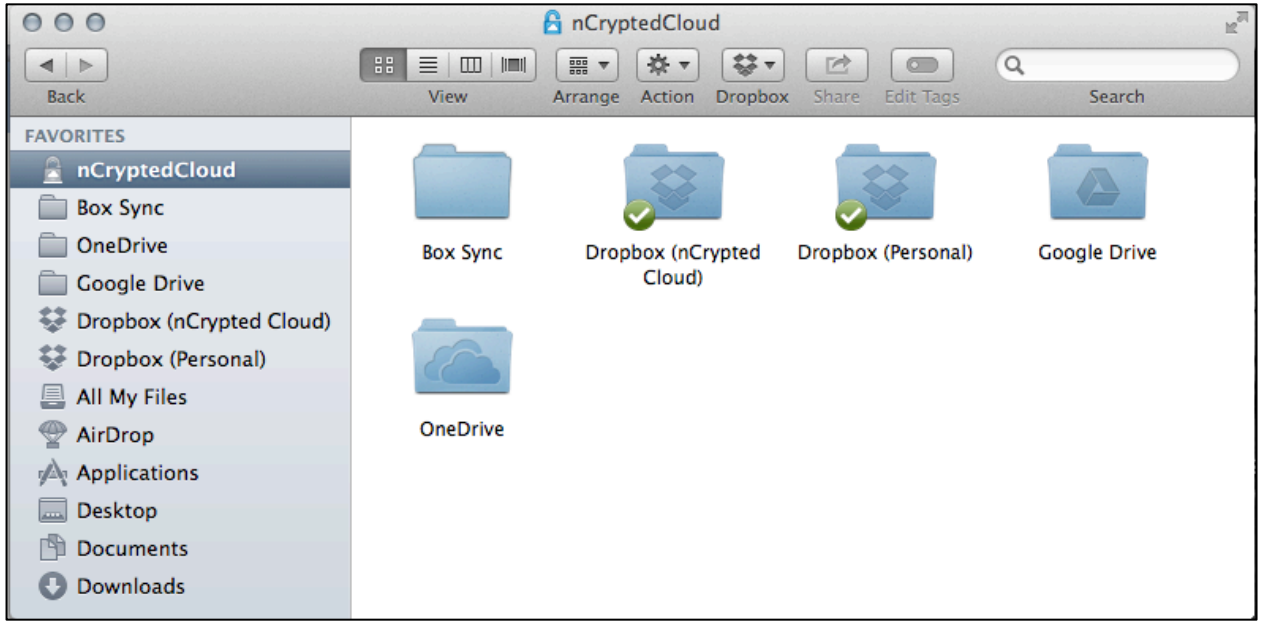
Once your cloud is detected, you will be prompted to sign-in to your cloud and grant access to it.





Cloud Storage 3.2

Once these cloud providers are synced, they will show appear in nCrypted Cloud's viewer. You will also have the ability to apply nCrypted Cloud settings to files and folders directly on the cloud provider's viewer.



Identities

4

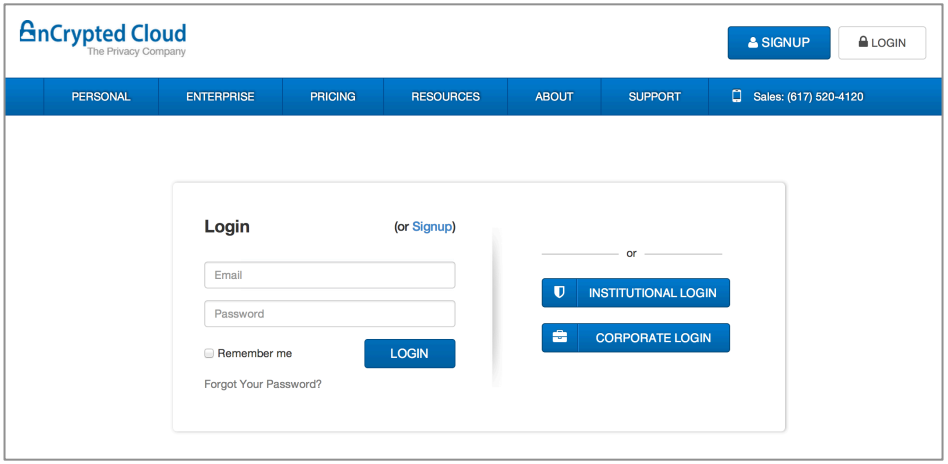
Identities
4.1

Add Corporate Identity

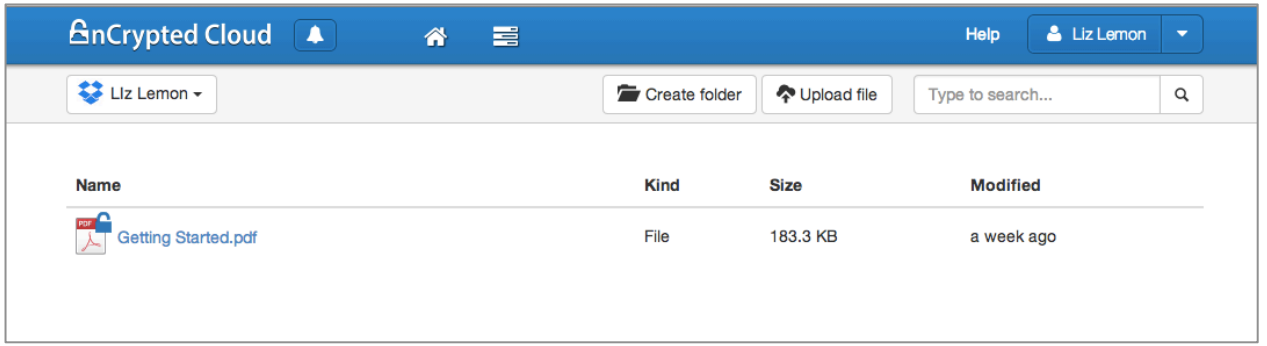
You can have one personal, and potentially many corporate identities with which you can manage and collaborate. Having multiple identities allows you to keep personal data separate from corporate data in the same cloud.

To add a corporate identity, you must do so on your **Cloud Web Portal.**

1. Go to www.ncryptedcloud.com/login and sign-in.

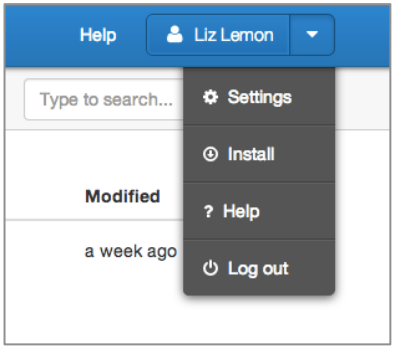


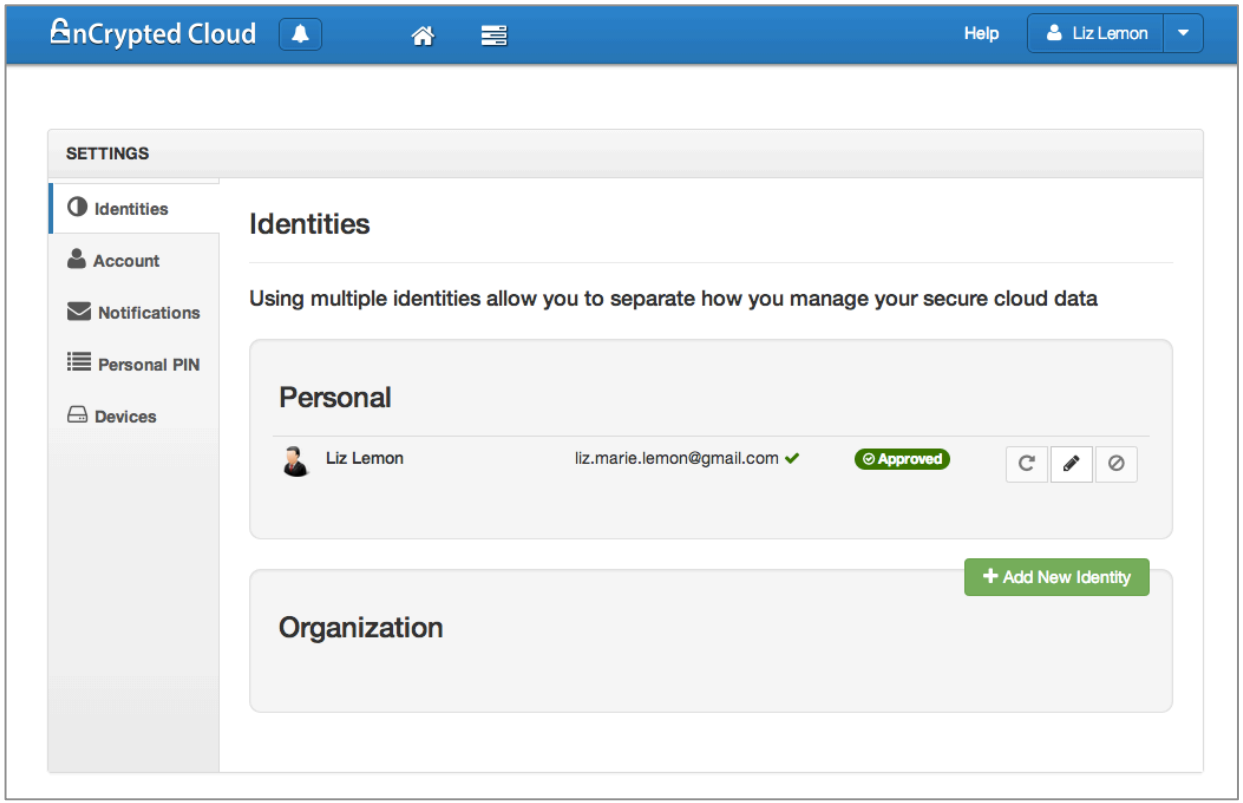
This is what your cloud web portal will look like.



Identities
4.1

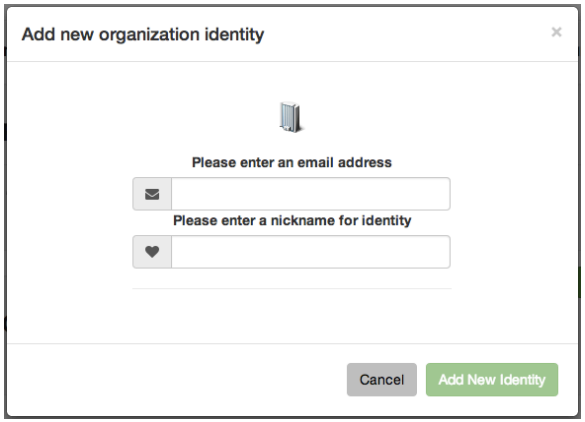
2. Click on the drop-down menu and select “Settings”. The ‘Identities’ tab is the first page you will see.



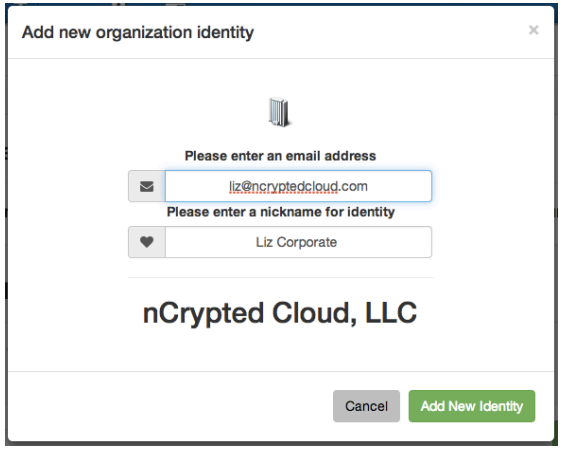


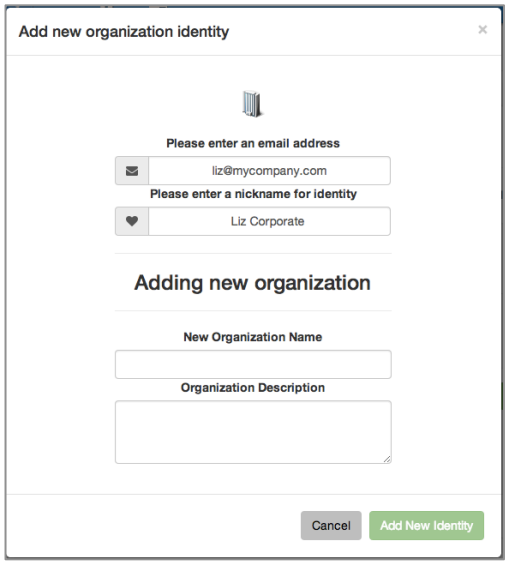
Identities
4.1

3. Click the green “Add New Identity” button under the Organization category and this pop-up will appear. Enter your organization email and a nickname for this identity.



4. If your organization is already registered with nCrypted Cloud, your corporate email address will be detected. If your organization is new to nCrypted Cloud, this pop-up window will expand and you will be asked to enter the name of your organization and a short description. Once you do so, nCrypted Cloud will receive this request and grant approval.



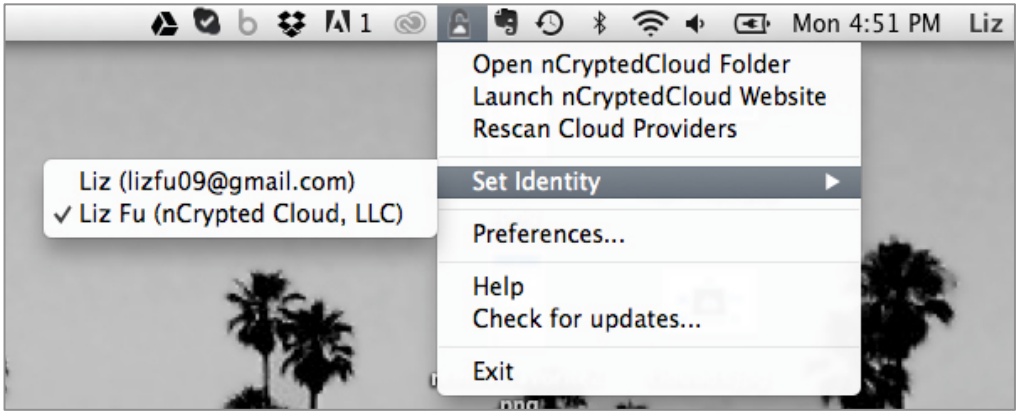


Identities
4.2

Switch Between Identities

Once your corporate email is approved, you will be able to switch between your personal and corporate identity on our desktop client.

1. Click on the nCrypted Cloud icon in your taskbar and select “Set Identity”.
2. You will see your identities. To switch between identities, click on the identity you wish to operate as.



If you are working under your corporate identity, a black briefcase icon will indicate that you are working with corporate files.

Secure

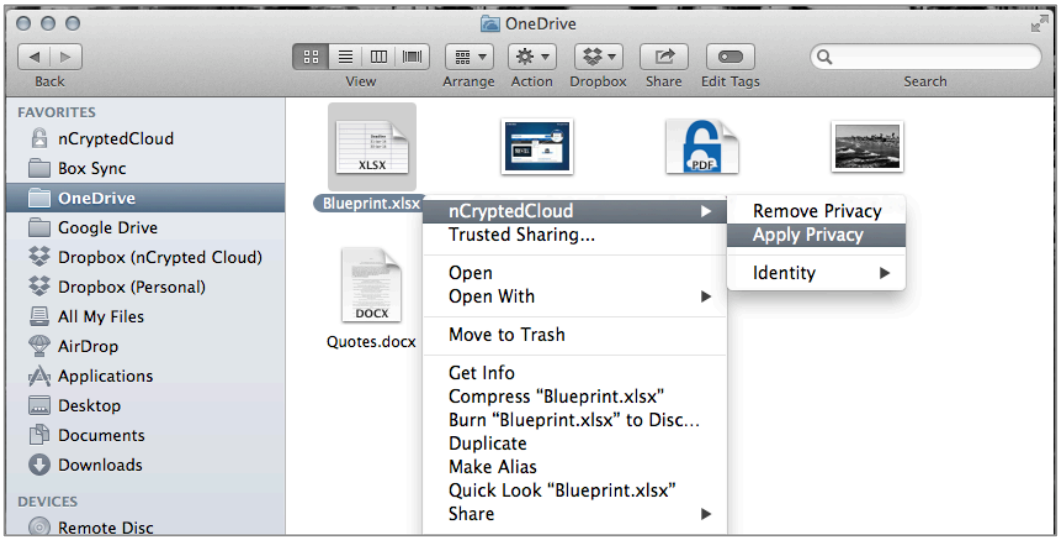
5

Secure
5.1

Make Private

nCrypted Cloud's Make Private feature gives you the ability to secure files with industry standard encryption technology (AES 256-bit encryption).

To make files and folders Private on your desktop, simply right-click the file or folder you wish to secure and select "Make Private".



A blue lock icon will appear on the secured file or folder. If you are working under your corporate identity, a briefcase icon will also appear on the top left corner of the file or folder.

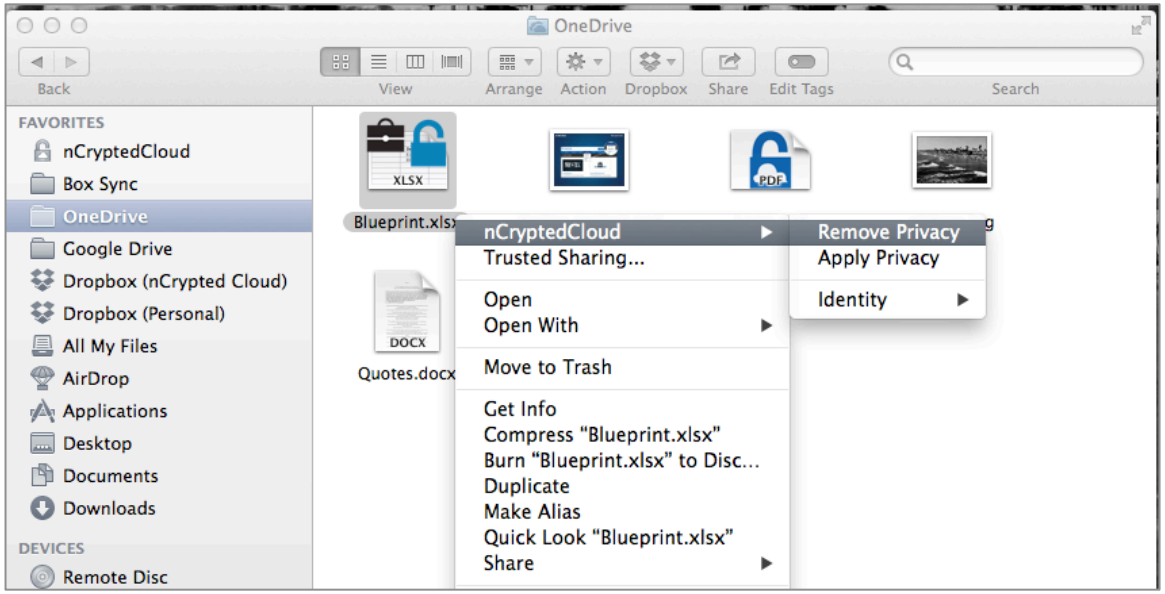
Blueprint.xlsx

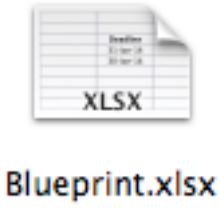
Blueprint.xlsx

Secure
5.2

Remove Privacy

To decrypt data, simply right click the file or folder and select “Remove Privacy”. The blue lock will disappear from the file or folder.





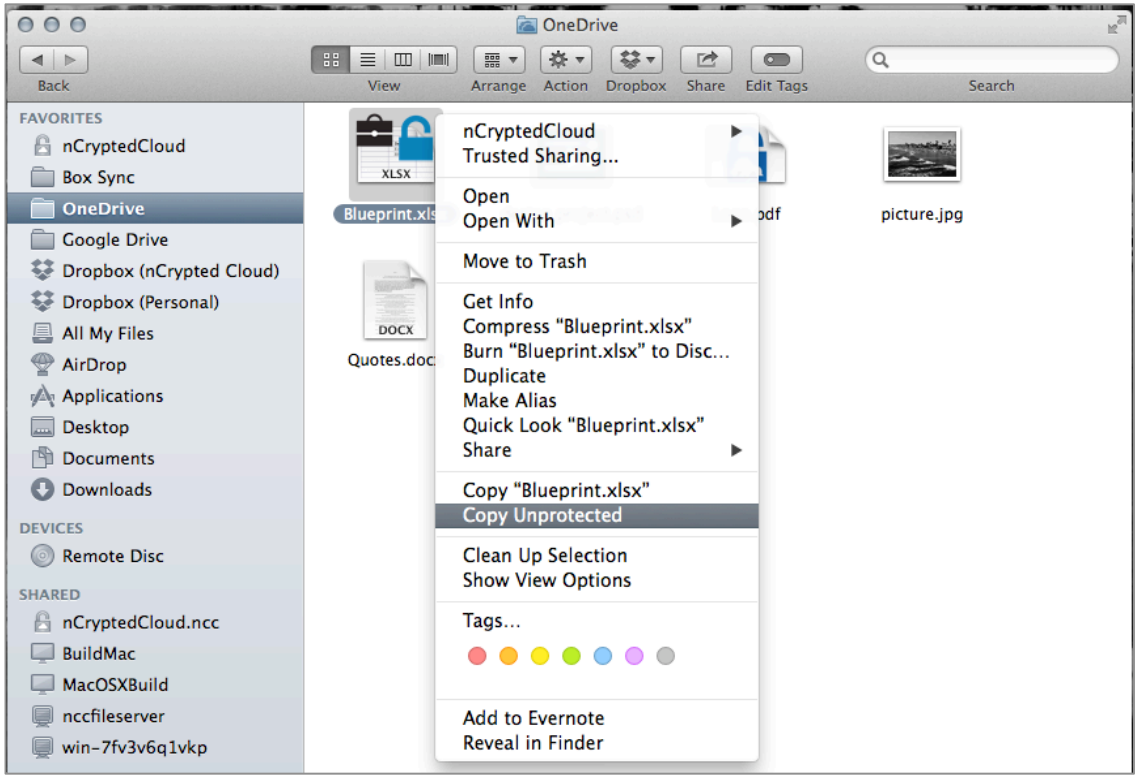
Secure
5.3

Copy Unprotected

This feature gives you the ability to copy encrypted files and paste them in their original file format (.doc, .xls, .pdf, .psd, etc.). When data is encrypted, its file format changes from its original file format to .zip format.

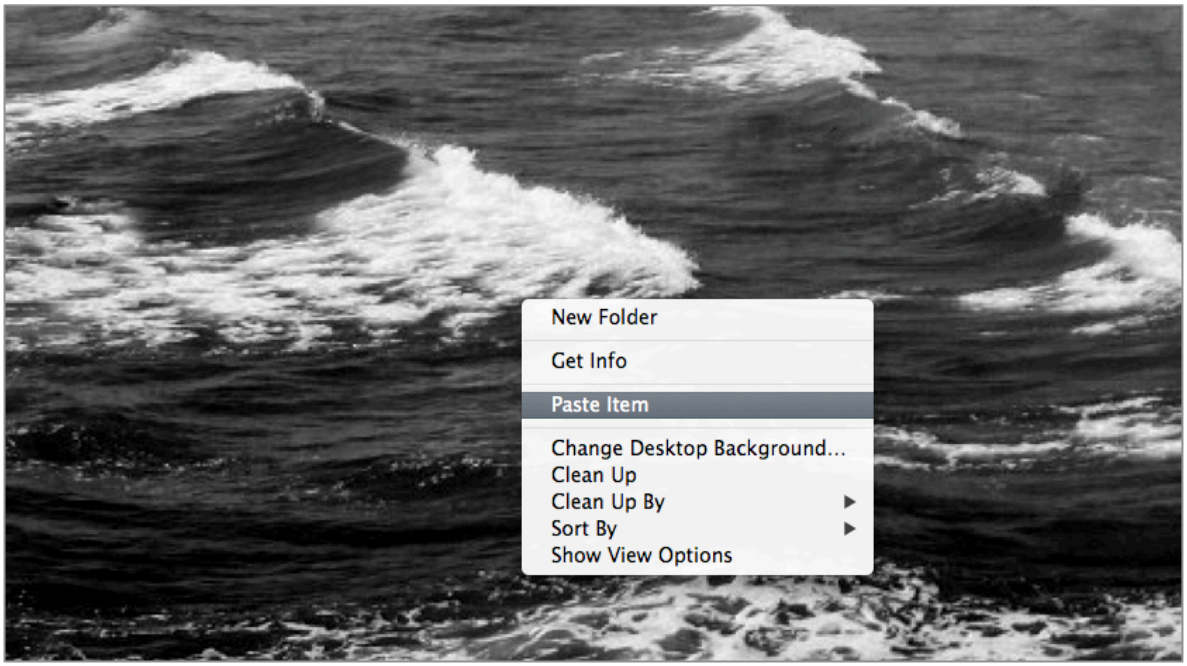
In order to ensure that your data is truly secure, it is encrypted no matter where it goes. If you copy an encrypted .zip file, it will be pasted as an encrypted .zip file and will not be accessible without nCrypted Cloud. This is where Copy Unprotected comes in.

To Copy Unprotected, right click the file or folder you wish to copy and select “Copy Unprotected”.

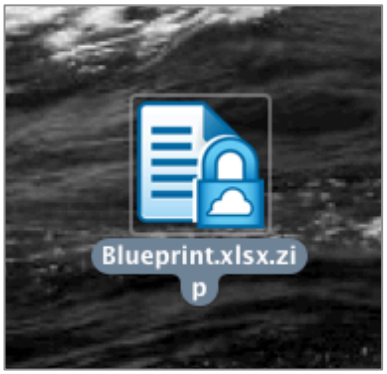


Secure 5.3

Paste the item you just Copy Unprotected.



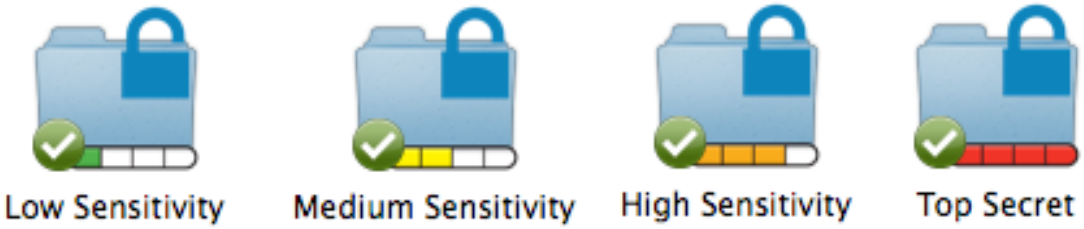
As you can see, the file was pasted in its original format (left). If you copied the file without using Copy Unprotected, the file will remain encrypted and in .zip format (right).



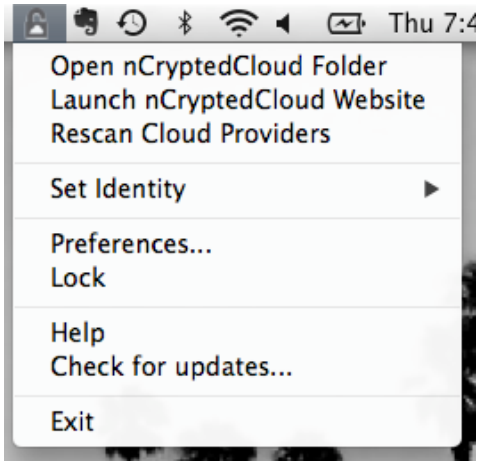
Secure 5.4

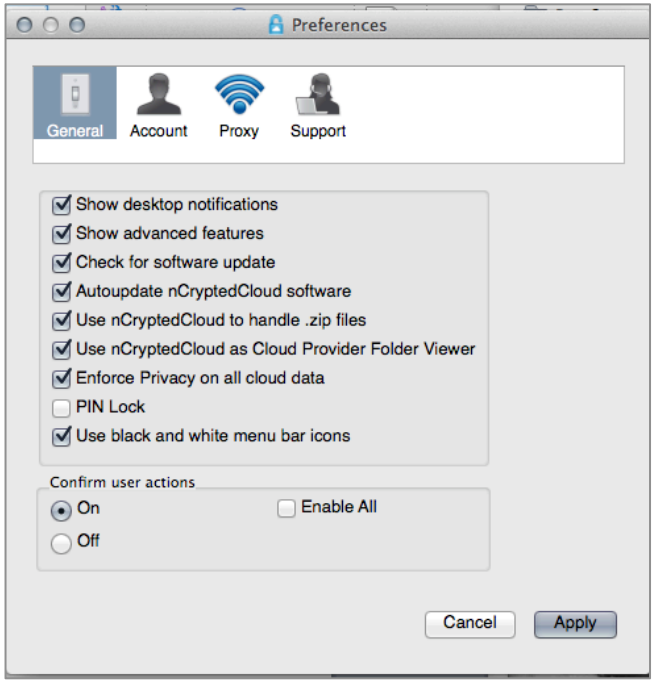
Apply Sensitivity

Sensitivity settings give you the ability to label folders based on how sensitive the files within the folder are. There are 4 sensitivity levels: Low, Medium, High, and Top Secret.



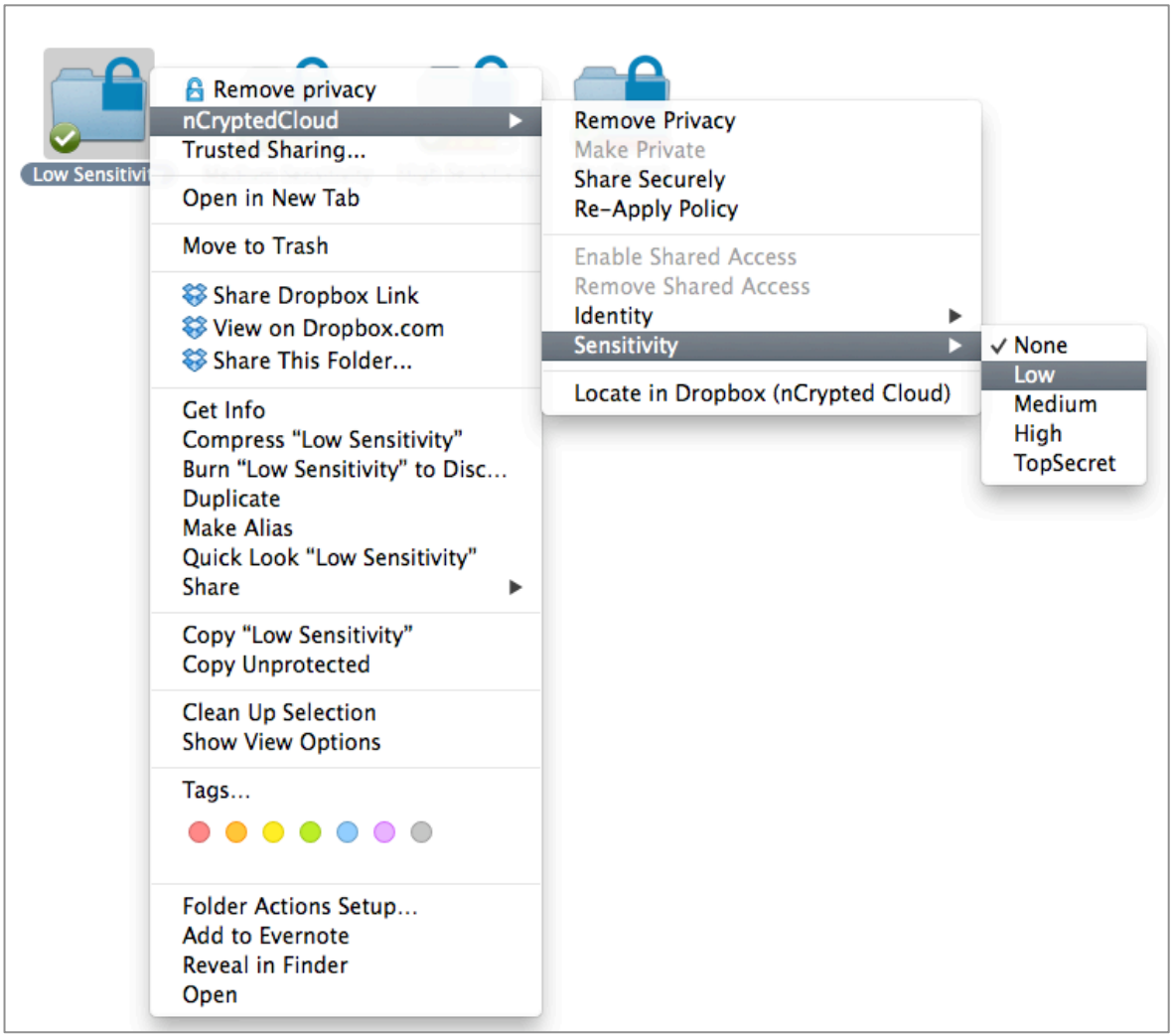
To apply sensitivity, make sure “Show Advanced Features” is checked in your Preferences Menu.





Secure 5.4

Once you enabled advanced settings, right-click the folder you wish to apply sensitivity to. Select "nCrypted Cloud" from the drop-down menu, then scroll over "Sensitivity". Here, you can choose the level of sensitivity you wish to apply to this folder.



Trusted Sharing

6

Trusted Sharing 6.1

Trusted Sharing Overview

Trusted Sharing gives you the ability to securely share files with anyone through nCrypted Cloud's secure web browser. This means that the recipient is not required to have cloud storage or an nCrypted Cloud account to securely access this file.

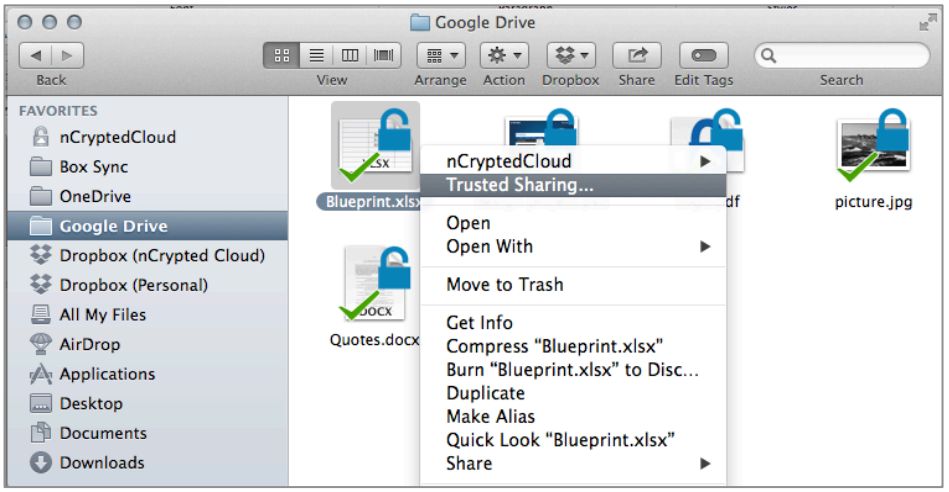
Here is a brief overview of how the Trusted Sharing Process works:

1. The sender sets specific Trusted Sharing permissions and shares the file/folder in the form of a link via email to the recipient.
2. The recipient receives the email with the link to the Trusted Share.
3. Once the recipient clicks on the link, the nCrypted Cloud secure web portal will open and the recipient will be able to access the file.
4. Once the recipient accesses the file, the sender will receive an email notifying them that the recipient has accessed the file/folder. This email will also contain a link manage the settings of the Trusted Share via the Share Management Page on the Cloud Web Portal.
5. The sender will also receive email notifications whenever the recipient makes any changes to data.
6. Once the link expires, the recipient will no longer have access to this Trusted Share.

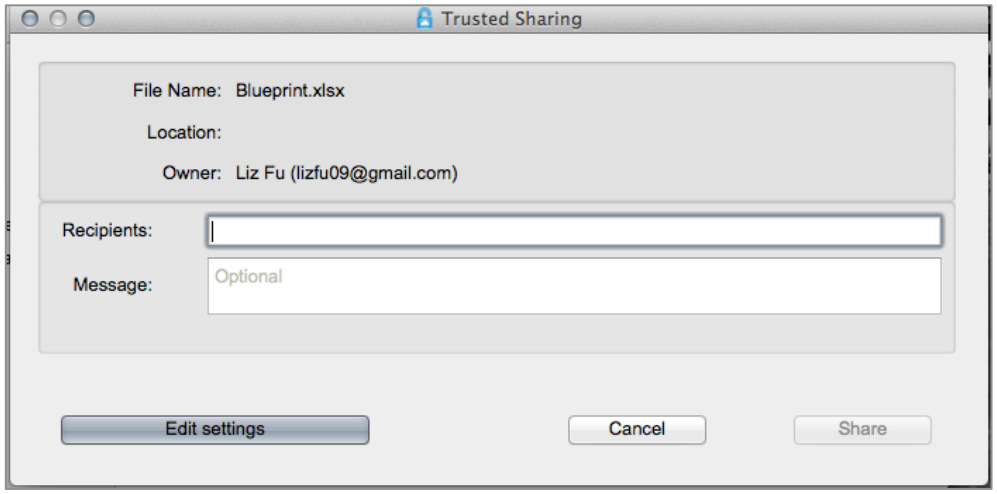
Trusted Sharing 6.1

How To Trusted Share

1. Right-click on the file you wish to share and select “Trusted Sharing.

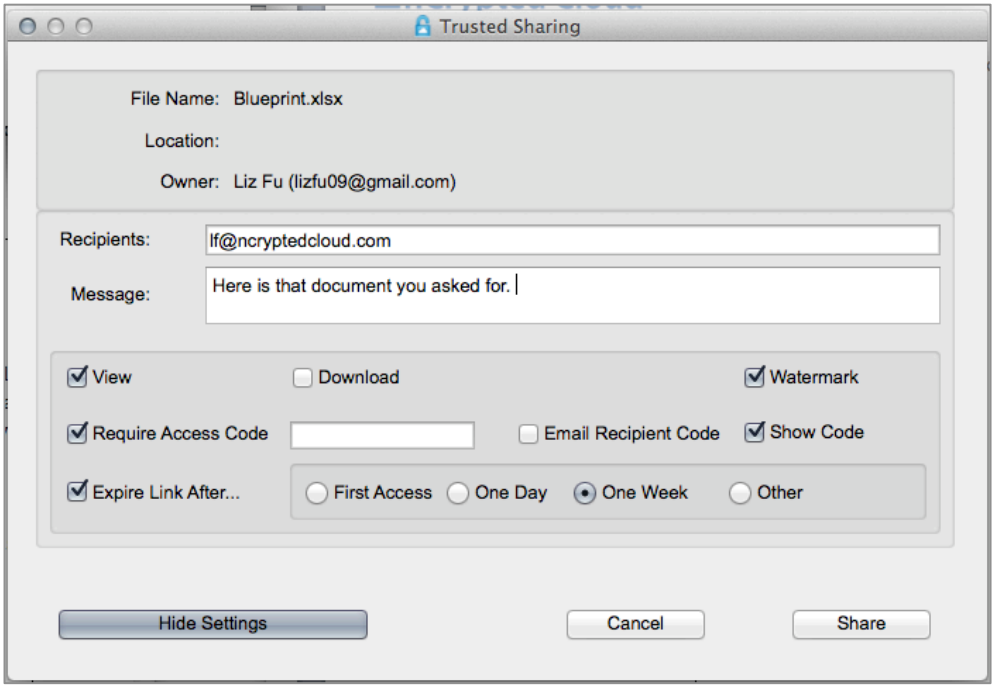


2. A pop-up window will appear. Enter the recipients’ email addresses and an optional message to go along with the Trusted Share.



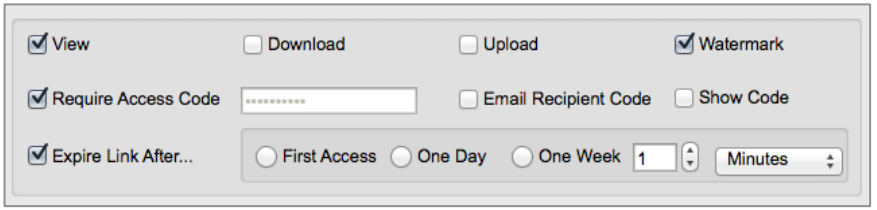
Trusted Sharing 6.1

3. Click “Edit Settings” to expand the menu and view more Trusted Sharing options.



4. The “View” and “Download” checkboxes give the recipient permission to either View Only, Download Only, or View and Download if both boxes are selected.

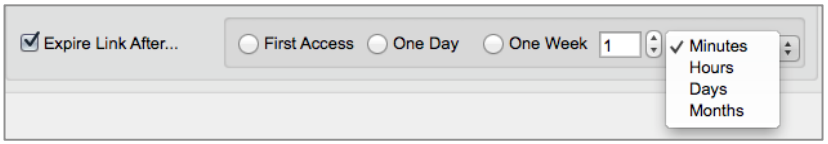
   If you are Trusted Sharing a **Folder**, you will see an additional “Upload” checkbox. This option allows you to securely ***receive*** files from recipients. If you check the box next to “Upload”, but not “View” and “Download”, the recipient only has permission to upload files into this folder, and cannot view the contents within.



Trusted Sharing 6.1

5. The Watermark checkbox gives you the option to watermark your file with the recipient's email and IP address. This is what a watermarked file looks like.

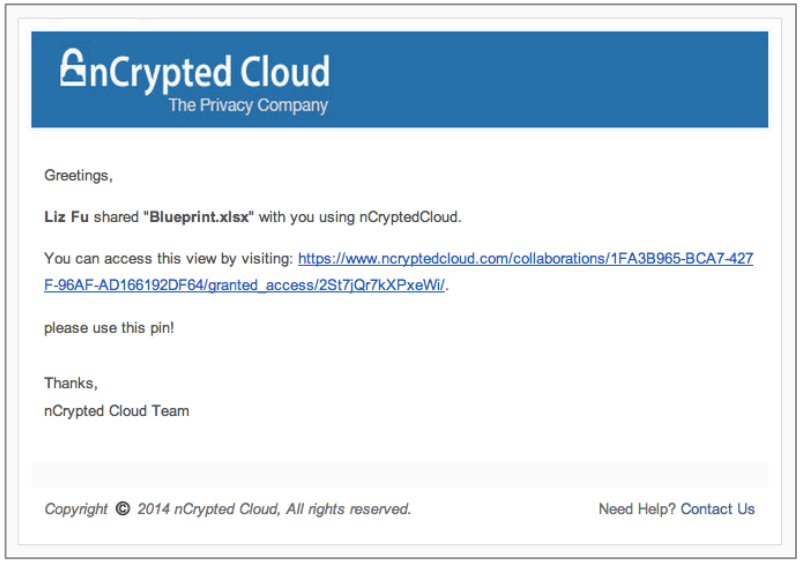
6. The Require Access Code option gives you the ability to require a passcode to access the Trusted Share. This access code can be sent to the recipient in an email, or not at all.
7. The Link Expiration option gives you to limit the amount of time your Trusted Sharing link is available for. If you click 'Other', you can set a specific time for your Trusted Share.



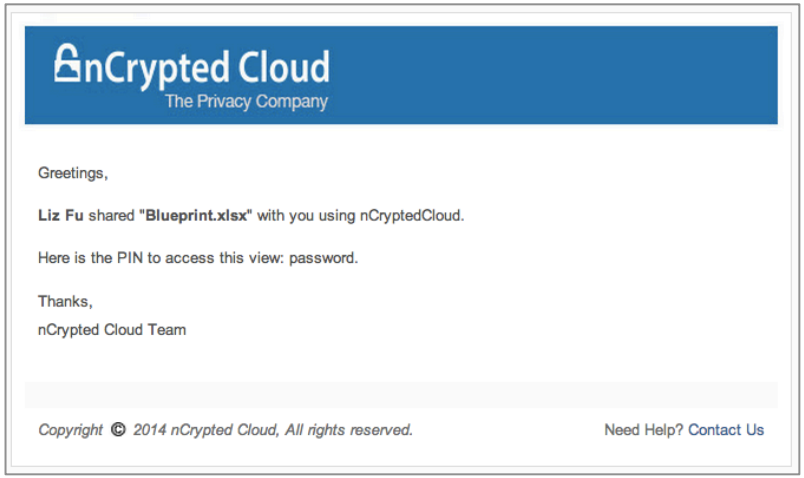
Trusted Sharing 6.2

Trusted Share Sent

Once you hit “Share”, a link to your file or folder will be sent to the recipient via email. This is the email they will receive.

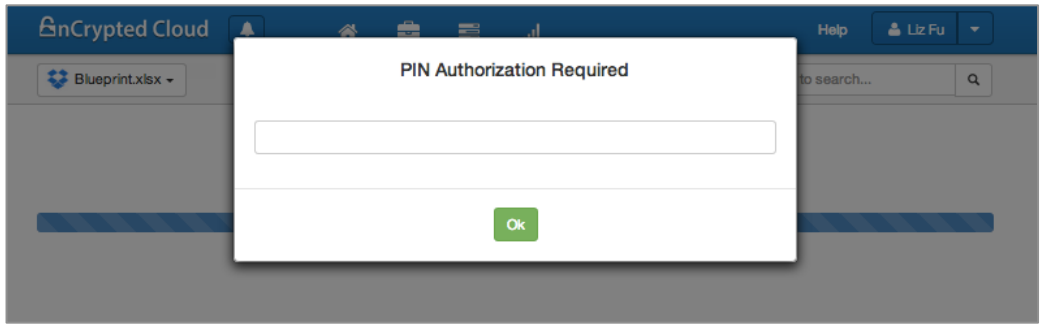

nCrypted Cloud
The Privacy Company
Greetings,
Liz Fu shared "Blueprint.xlsx" with you using nCryptedCloud.
You can access this view by visiting: https://www.ncryptedcloud.com/collaborations/1FA3B965-BCA7-427F-96AF-AD166192DF64/granted_access/2St7jQr7kXPxeWi/.
please use this pin!
Thanks,
nCrypted Cloud Team
Copyright © 2014 nCrypted Cloud, All rights reserved.
Need Help? Contact Us

If you sent the recipient the access code through email, this is the second email they will receive.

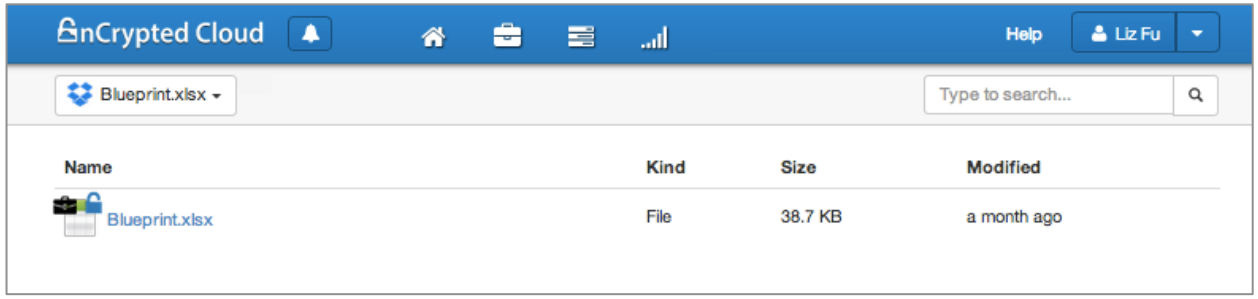

nCrypted Cloud
The Privacy Company
Greetings,
Liz Fu shared "Blueprint.xlsx" with you using nCryptedCloud.
Here is the PIN to access this view: password.
Thanks,
nCrypted Cloud Team
Copyright © 2014 nCrypted Cloud, All rights reserved.
Need Help? Contact Us

Trusted Sharing 6.2

Once the recipient click on the first initial link, they must enter a PIN code in order to proceed.

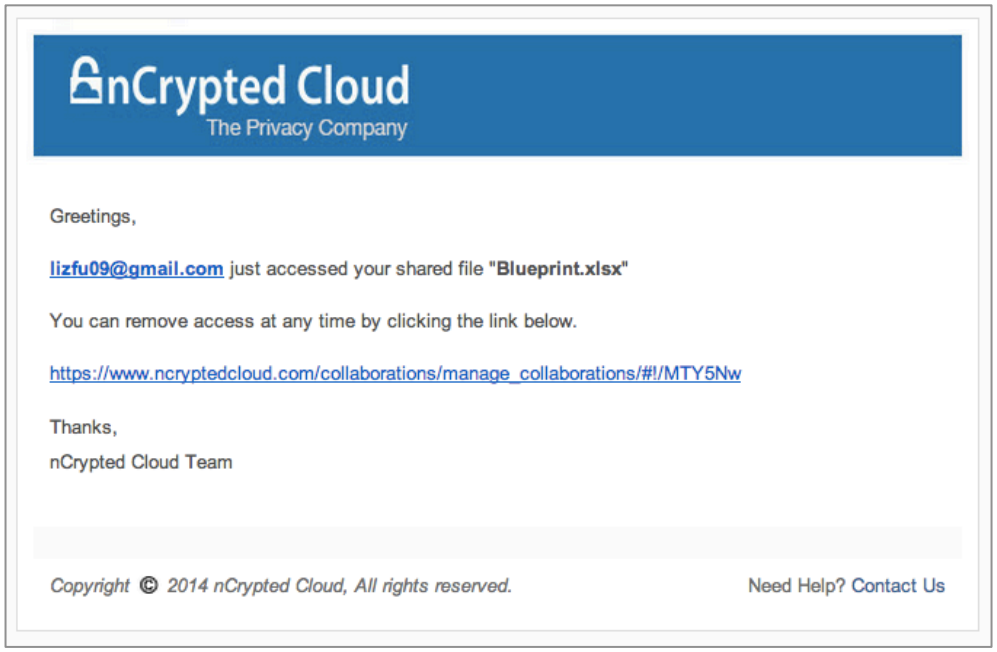


Once they do so, they will be able to access the file or folder by clicking on the document name in nCrypted Cloud's secure web browser.

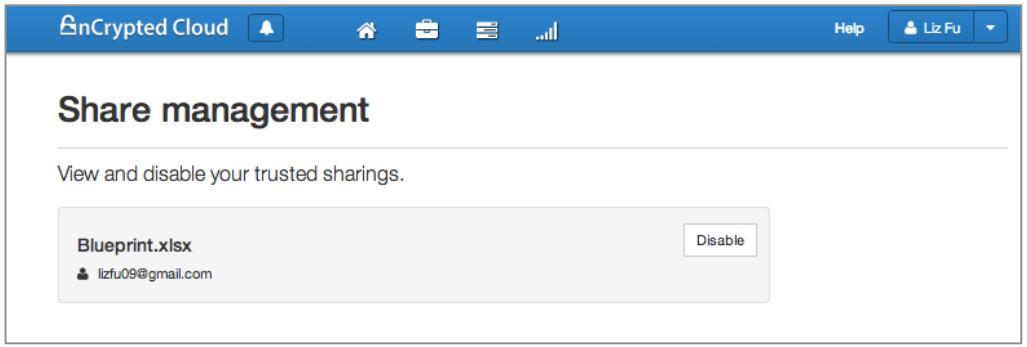


Trusted Sharing 6.2

Once the recipient accesses your Trusted Share, this is the email you will receive.

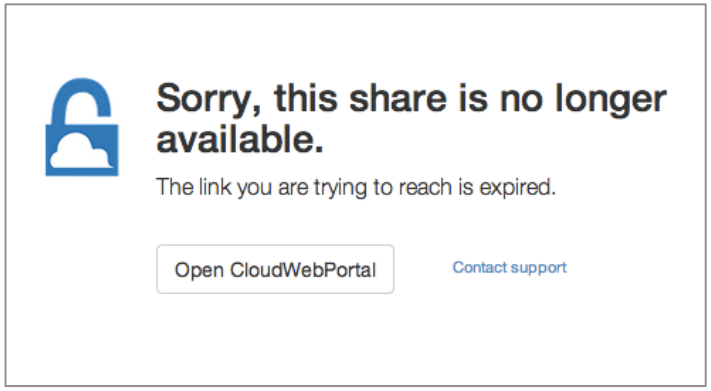

nCrypted Cloud
The Privacy Company
Greetings,
lizfu09@gmail.com just accessed your shared file "Blueprint.xlsx"
You can remove access at any time by clicking the link below.
https://www.ncryptedcloud.com/collaborations/manage_collaborations/#!/MTY5Nw
Thanks,
nCrypted Cloud Team
Copyright © 2014 nCrypted Cloud, All rights reserved.
Need Help? Contact Us

If you click on the link within the email, you be redirected to the Share Management Page on the Cloud Web Portal where you will be able to disable access to this Trusted Share.



Trusted Sharing 6.2

Once you disable access, this is what the recipient will see when they click on the Trusted Sharing link in their email.


Sorry, this share is no longer available.
The link you are trying to reach is expired.
Open CloudWebPortal
Contact support

Share Securely

7

Share Securely 7.1

Share Securely Overview

Another way you can share data is through nCrypted Cloud's Share Securely feature. While Trusted Sharing is geared more towards temporary shares on a one-off basis, share securely is intended for extended collaboration purposes.

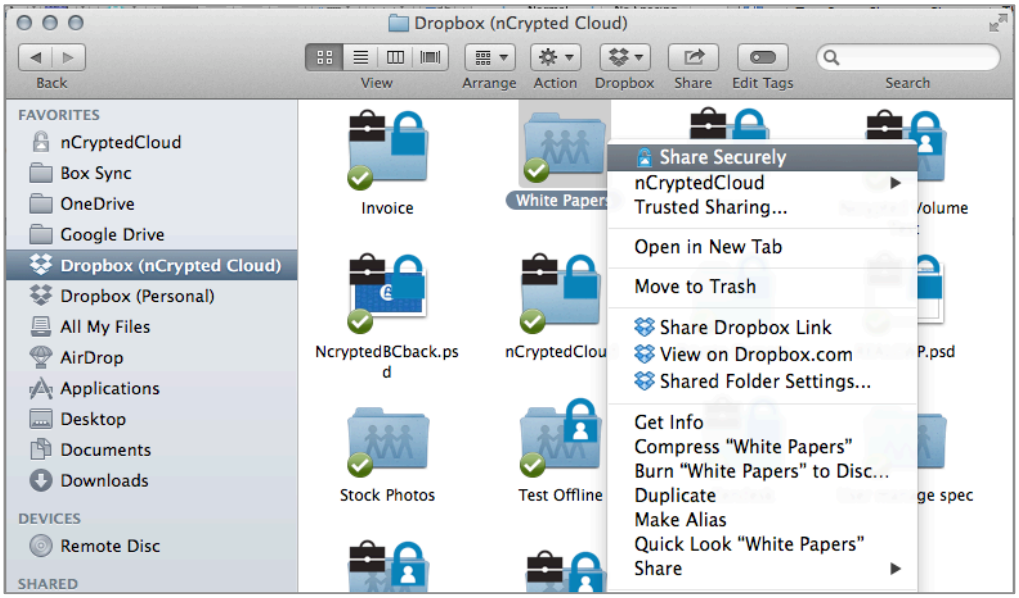
Unlike Trusted Sharing, Share Securely requires that the recipient of a shared folder have a cloud storage account and an nCrypted Cloud account. Folders are shared just as they normally are through native cloud storage providers (Dropbox, Google Drive, One Drive, Box, Egnyte, etc.) and privacy is applied to these shared folders through nCrypted Cloud.

Once a folder is "Shared Securely", all shared members must have nCrypted Cloud installed in order to access the encrypted files within the folder.

Share Securely 7.1

How To Share Securely

To Share Securely, simply right-click the folder you wish to share and select “Share Securely”.

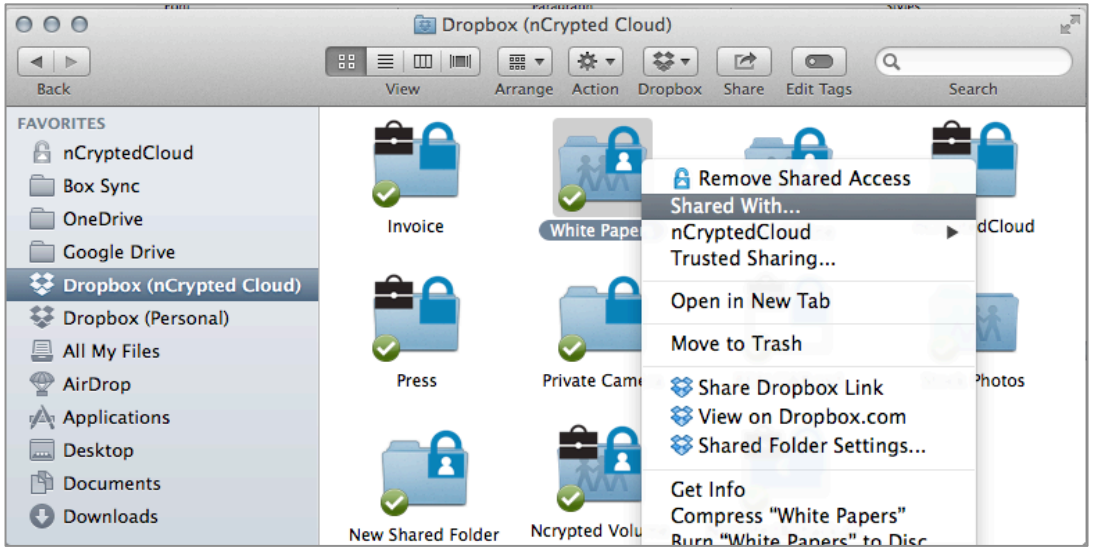


A blue lock icon with a person inside of it will appear at the top right corner of the folder.

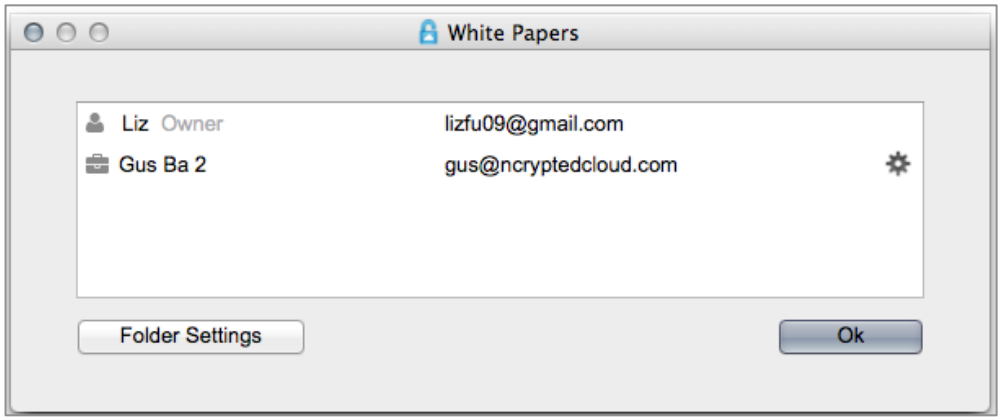
Share Securely 7.2

View Shared With

You can view the users this folder is shared with by right-clicking the folder and selecting “Shared With”.



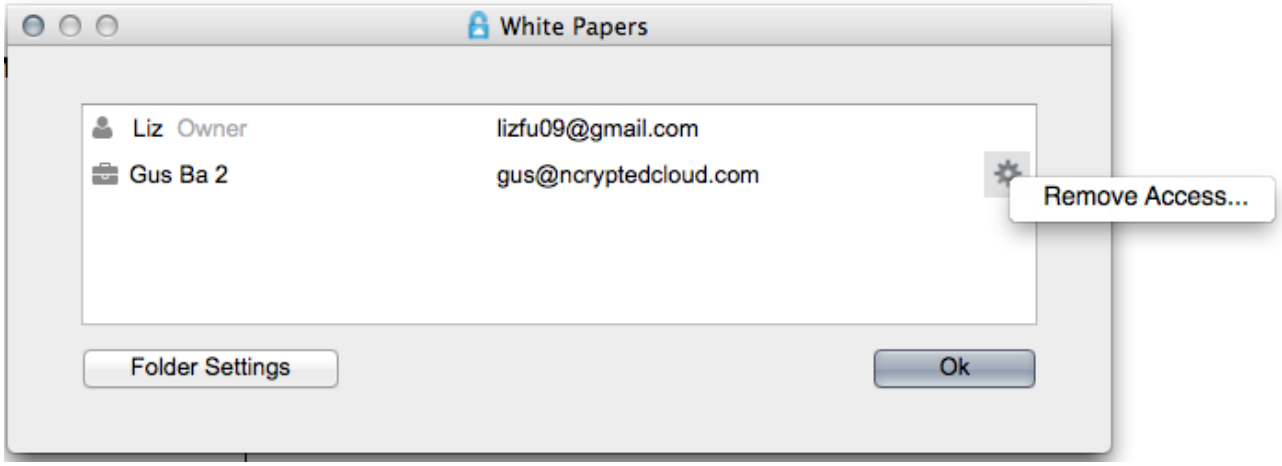
A pop-up window will appear with a list of the names and email addresses of this folder’s shared users.



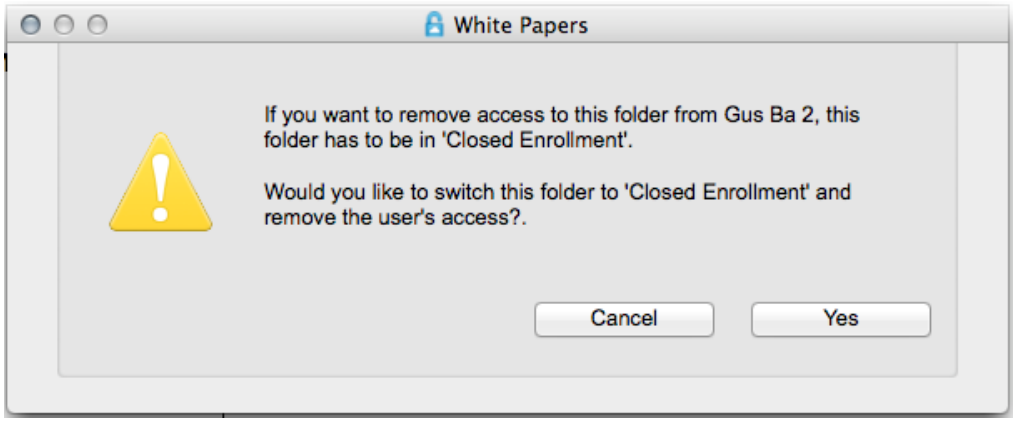
Share Securely
7.3

Remove User Access

Right from this screen, you can remove user access to this shared folder by clicking on the settings icon on the right of the user's name and email address.



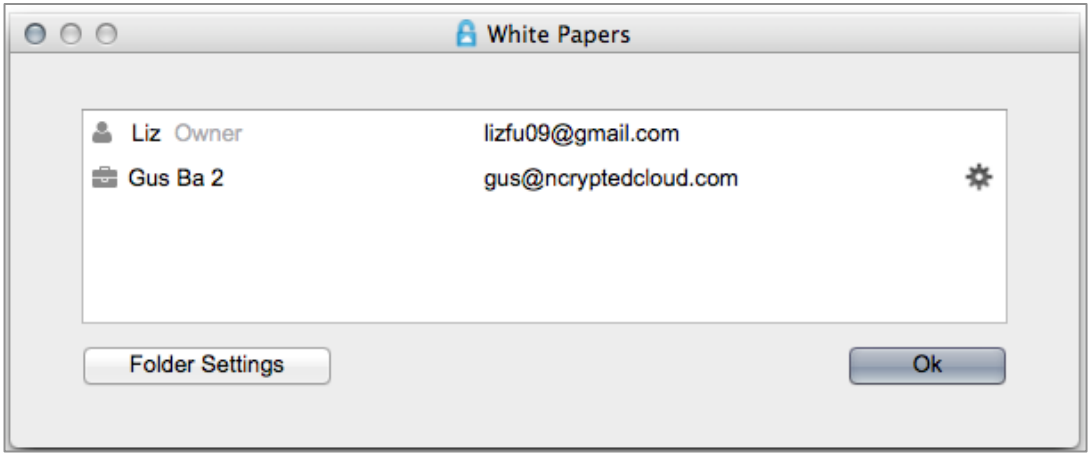
Once you select Remove Access, this is the pop-up that will appear. Click "Yes" to remove access from this user. The following pages will discuss Open and Closed Enrollment.


White Papers
If you want to remove access to this folder from Gus Ba 2, this folder has to be in 'Closed Enrollment'.
Would you like to switch this folder to 'Closed Enrollment' and remove the user's access?.
Cancel
Yes

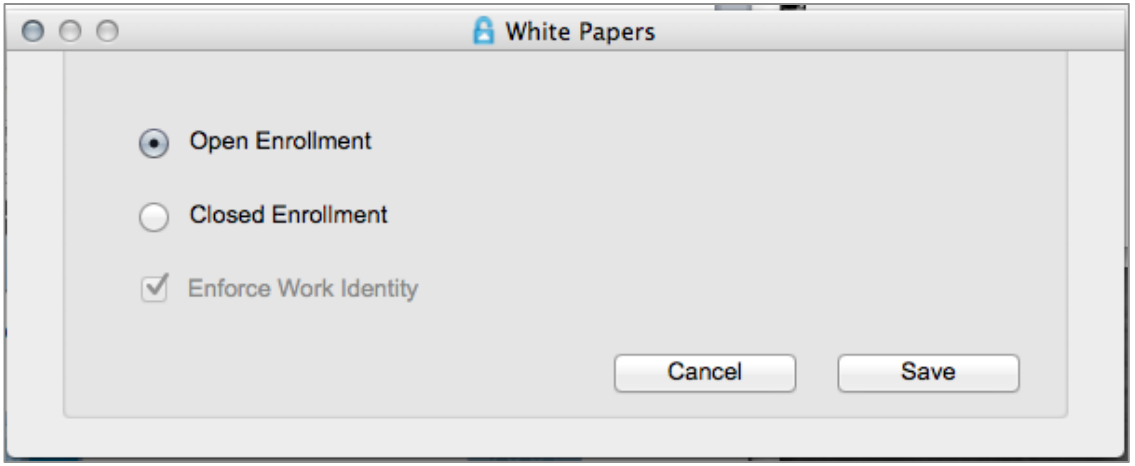
Share Securely
7.4

Open + Closed Enrollment

Open and Closed Enrollment options give you the ability to control access to folders based on identity settings. You can adjust Open and Closed Enrollment settings by clicking on the “Folder Settings” button on your Shared With pop-up window.



This is what you will see.



Share Securely 7.4

There are 4 types of Open and Closed Enrollment Situation:

Open Enrollment (Allow-by-Default): Anyone who has the folder in his/her cloud can access the folder.

Closed Enrollment (Deny By Default): The only people who can access the folder are those whom the folder is directly shared with. If a user's name does not appear on the "Shared With" List, the user does not have access to that folder. However, users without access still have the ability to request access. Ultimately, the only person who can approve and deny access is the file owner.

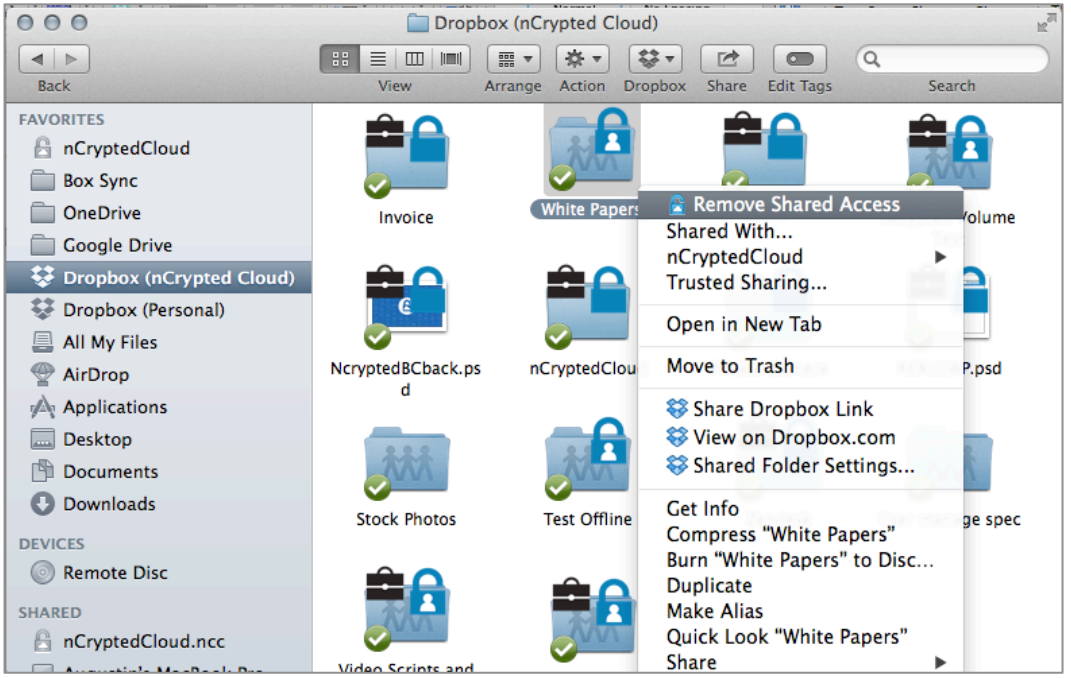
Open Enrollment With Enforced Work Identity: In this situation, anyone who falls under the same work identity and has the folder in his/her cloud, by default, can access the folder. However, if the user does not fall under the same work identity, access can still be granted if they choose to request access.

Closed Enrollment With Enforced Work Identity: This situation requires two criteria for folder access: the user must fall under the same corporate organization and must also have the folder directly shared. If both these criteria are not met, access is denied.

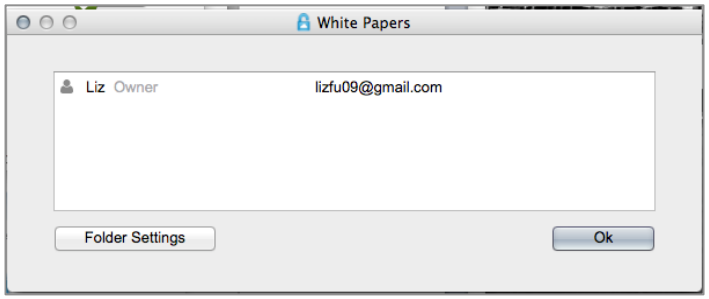
Share Securely 7.5

Remove Shared Access

You can remove shared access of a shared folder by right clicking the folder Shared Securely and clicking “Remove Shared Access”.

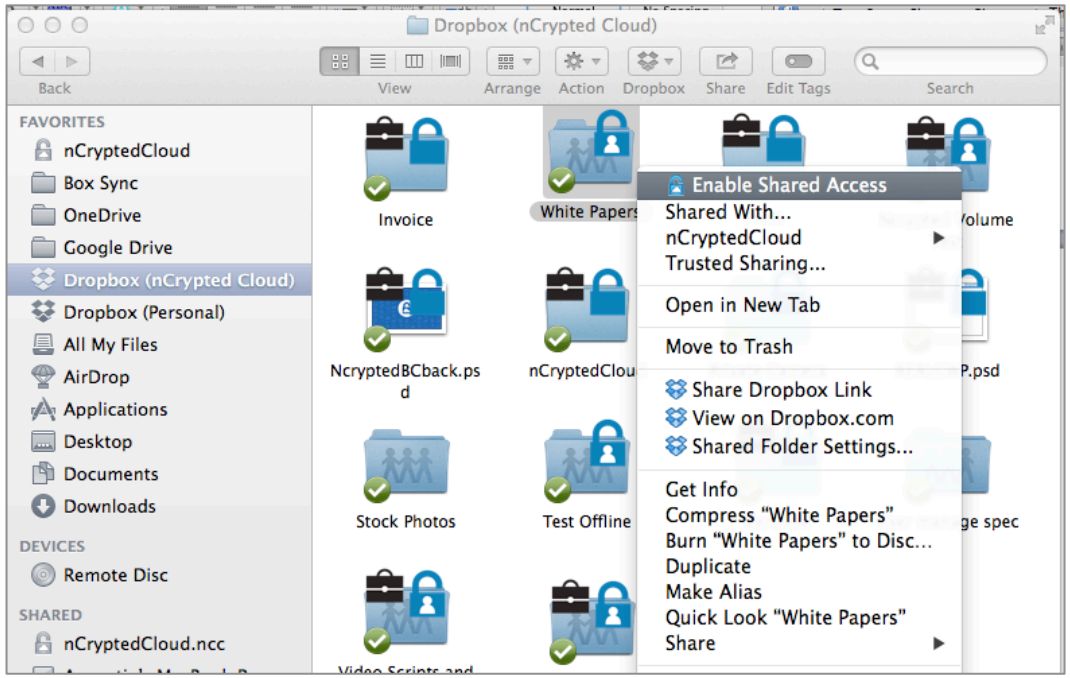


Access to this folder will be removed.



Enable Shared Access

If you remove shared access and want to re-enable it, you can by right-clicking the shared folder and selecting “Enable Shared Access”.



Shared access to this folder has now been re-enabled.

Auditing

8

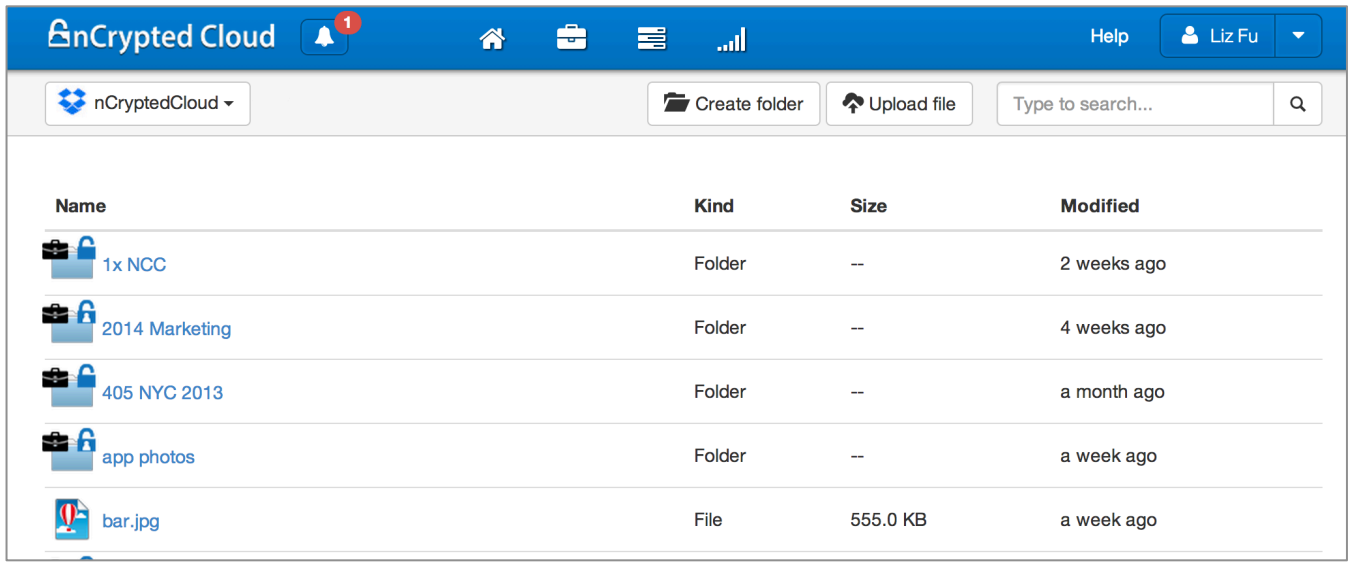
Auditing 8.1

View Auditing Events

nCrypted Cloud's Auditing feature gives you the ability to keep track of all data activity. This means that you have the ability to keep track of what data was accessed, who accessed the data, when they did it, what they did, and from what device.

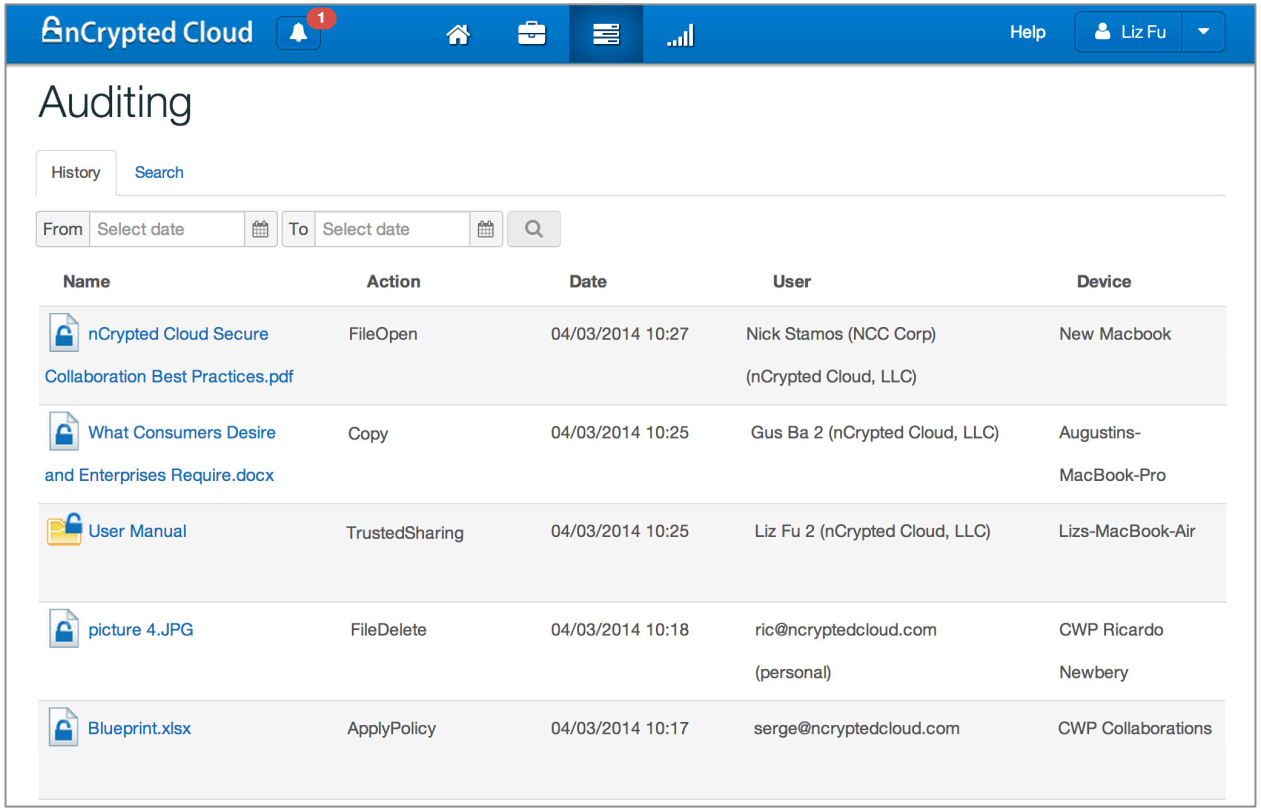
The Auditing Page can be found on your Cloud Web Portal.

To access your personal auditing page, go to www.ncryptedcloud.com/login and log into your account. You will be directed to your Cloud Web Portal.



Auditing
8.1

Click on the three bar icon in your top bar and your auditing page will open.



This page will give you the name of the file or folder being accessed, what action was performed on this file or folder, the date it occurred, the user that performed the action, and the device that was used.